

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-50745

(P2003-50745A)

(43) 公開日 平成15年2月21日 (2003.2.21)

(51) Int.Cl. ⁷	識別記号	F I	テーム [*] (参考)
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 B 5 B 0 1 7
			3 2 0 F 5 J 1 0 4
17/60	1 4 2	17/60	1 4 2
	3 0 2		3 0 2 E
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 D
審査請求 未請求 請求項の数17 O L (全 66 頁)			

(21) 出願番号 特願2001-239145(P2001-239145)

(22) 出願日 平成13年8月7日 (2001.8.7)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 浅野 智之

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(72) 発明者 村松 克美

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100101801

弁理士 山田 英治 (外2名)

Fターム(参考) 5B017 AA03 BA07 CA09 CA16

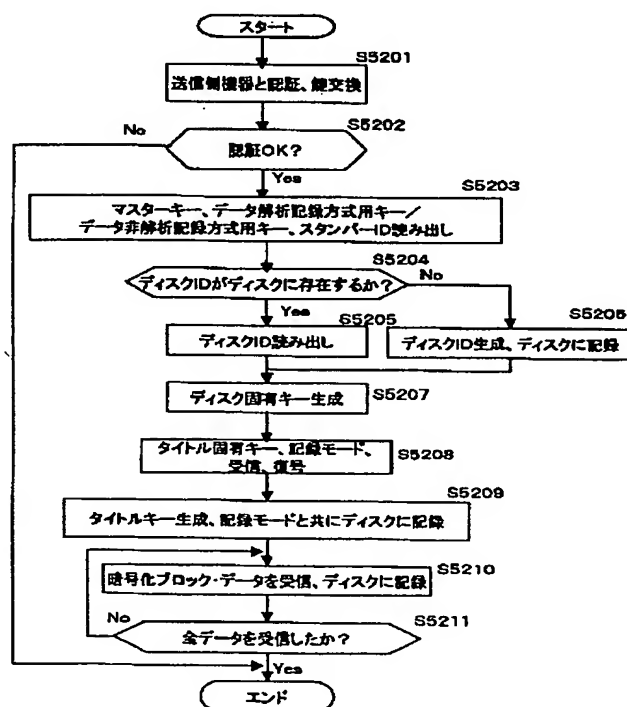
5J104 AA16 EA04 EA26 NA02 PA14

(54) 【発明の名称】 情報処理装置、および情報処理方法、並びにコンピュータ・プログラム

(57) 【要約】

【課題】 コンテンツの機器間コピーまたは配信コンテンツの格納における効率的処理を実現した処理構成を提供する。

【解決手段】 コンテンツを情報記録再生装置間においてコピーまたは移動する際、あるいは配信コンテンツを情報記録再生装置の記録媒体に格納する際、コンテンツの復号、再暗号化なしに記録媒体に格納するとともに、タイトル固有キーをデータ送信側から入力し、入力タイトル固有キーに基づいてタイトルキーを生成して、記録媒体に格納する。データ再生時は、自己のマスターキー、メディアキー、LSIキー等と、格納したタイトルキーに基づくタイトル固有キー生成シーケンスに従って、タイトル固有キーを生成し、データの復号、再生を行なう。



【特許請求の範囲】

【請求項1】情報の暗号処理を実行する暗号処理手段を有する情報処理装置であり、

前記暗号処理手段は、

予め設定された暗号処理シーケンスに従って鍵を生成し、生成した鍵を適用して記録媒体に格納された暗号データの復号処理を実行する構成を有するとともに、記録媒体格納処理対象データとして外部から入力する入力暗号データに対応して設定された第1暗号鍵に対して、前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理を実行して第2暗号鍵を生成する処理を実行し、

前記第2暗号鍵を適用した前記暗号処理シーケンスの実行により前記入力暗号データの復号用鍵を生成する処理を実行する構成を有することを特徴とする情報処理装置。

【請求項2】前記暗号処理シーケンスは、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかを適用した暗号処理として実行される暗号処理シーケンスであり、前記入力暗号データの復号用鍵の生成においては、前記第2暗号鍵と、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかを適用した暗号処理シーケンスを実行する構成であることを特徴とする請求項1に記載の情報処理装置。

【請求項3】前記第1暗号鍵は、外部から入力する前記入力暗号データとしてのコンテンツに対して設定されるタイトル固有キーであり、前記第2暗号鍵は、前記タイトル固有キーの復号処理により取得可能なタイトルキーであり、前記入力暗号データの復号用鍵は、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかの鍵と、前記タイトルキーとの双方を適用した暗号処理により生成される鍵であることを特徴とする請求項1に記載の情報処理装置。

【請求項4】前記情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを格納し、前記暗号処理手段は、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含まれるキーにより暗号化した有効化キーブロック（EKB）の復号処理を実行し、該複合処理によって取得可能な鍵と、前記第2暗号鍵とを適用して前記前記暗号処理シーケンスを実行して前記入力暗号データの復号用鍵を生成する処理を実行する構成を有することを特徴とする請求項1に記載の情報処理装置。

【請求項5】前記入力暗号データは、トランスポートストリームを構成するパケットからなるブロックデータとして入力され、

前記暗号処理手段は、前記第2暗号鍵を適用して、前記復号用鍵としての各ブロックデータに対応するブロックキーの生成処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

【請求項6】前記暗号処理手段は、前記前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理による前記第2暗号鍵の生成処理、または、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行において、適用鍵の鍵長を変更する縮合処理または伸長処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

【請求項7】前記暗号処理手段は、外部から入力する入力暗号データの入力処理に際して、データ送信装置との認証処理を実行し、認証の成立を条件として、入力暗号データの入力処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

【請求項8】前記情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを格納し、前記暗号処理手段は、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含まれるキーにより暗号化した有効化キーブロック（EKB）の復号処理を実行し、該複合処理によって前記第1暗号鍵の取得処理を実行する構成であることを特徴とする請求項1に記載の情報処理装置。

【請求項9】情報の暗号処理を実行する情報処理方法であり、

予め設定された暗号処理シーケンスに従って鍵を生成し、生成した鍵を適用して記録媒体に格納された暗号データの復号処理を実行するステップと、記録媒体格納処理対象データとして外部から入力する入力暗号データに対応して設定された第1暗号鍵に対して、前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理を実行して第2暗号鍵を生成するステップと、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行により前記入力暗号データの復号用鍵を生成する処理を実行するステップと、を有することを特徴とする情報処理方法。

【請求項10】前記暗号処理シーケンスは、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかを適用した暗号処理として実行される暗号処理シーケンスであり、前記入力暗号データの復号用鍵の生成においては、前記第2暗号鍵と、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかを適用した暗号処理シーケンスを実行することを特徴とする請求項9に記載の情報処理方法。

【請求項11】前記第1暗号鍵は、外部から入力する前

記入入力暗号データとしてのコンテンツに対して設定されるタイトル固有キーであり、

前記第2暗号鍵は、前記タイトル固有キーの復号処理により取得可能なタイトルキーであり、

前記入入力暗号データの復号用鍵は、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかの鍵と、前記タイトルキーとの双方を適用した暗号処理により生成される鍵であることを特徴とする請求項9に記載の情報処理方法。

【請求項12】前記情報処理方法を実行する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを有し、前記入入力暗号データの復号用鍵を生成するステップにおいて、

ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（EKB）の復号処理を実行し、該複合処理によって取得可能な鍵と、前記第2暗号鍵とを適用して前記前記暗号処理シーケンスを実行して前記復号用鍵を生成する処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項13】前記入入力暗号データは、トランスポートストリームを構成するパケットからなるブロックデータとして入力され、

前記第2暗号鍵を適用して、前記復号用鍵としての各ブロックデータに対応するブロックキーの生成処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項14】前記前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理による前記第2暗号鍵の生成処理、または、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行において、適用鍵の鍵長を変更する縮合処理または伸長処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項15】前記情報処理方法において、さらに、外部から入力する入力暗号データの入力処理に際して、データ送信装置との認証処理を実行し、認証の成立を条件として、入力暗号データの入力処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項16】前記情報処理方法を実行する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを有し、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック

（EKB）の復号処理を実行し、該複合処理によって前記第1暗号鍵の取得処理を実行することを特徴とする請求項9に記載の情報処理方法。

【請求項17】情報の暗号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであつ

て、予め設定された暗号処理シーケンスに従って鍵を生成し、生成した鍵を適用して記録媒体に格納された暗号データの復号処理を実行するステップと、記録媒体格納処理対象データとして外部から入力する入力暗号データに対応して設定された第1暗号鍵に対して、前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理を実行して第2暗号鍵を生成するステップと、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行により前記入入力暗号データの復号用鍵を生成する処理を実行するステップと、を具備することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関し、さらに詳細には、著作権保護等、利用制限の付加されたコンテンツの機器間の移動、複製処理、あるいは通信媒体から機器への移動、複製処理を、利用制限を考慮し、かつ効率的に実行する情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。

【0002】

【従来の技術】デジタル信号処理技術の進歩、発展に伴い、近年においては、情報をデジタル的に記録する記録装置や記録媒体が普及しつつある。このようなデジタル記録装置および記録媒体によれば、例えば画像や音声を劣化させることなく記録、再生を繰り返すことができる。このようにデジタルデータは画質や音質を維持したまま何度もコピーを繰り返し実行することができるため、コピーが違法に行われた記録媒体が市場に流通することになると、音楽、映画等各種コンテンツの著作権者、あるいは正当な販売権者等の利益が害されることになる。昨今では、このようなデジタルデータの不正なコピーを防ぐため、デジタル記録装置および記録媒体に違法なコピーを防止するための様々な処理構成が実現または提案されている。

【0003】例えば、MD（ミニディスク）（MDは商標）装置において、違法なコピーを防止する方法として、SCMS（Serial Copy Management System）が採用されている。SCMSは、データ再生側において、オーディオデータとともにSCMS信号をデジタルインタフェース（DIF）から出力し、データ記録側において、再生側からのSCMS信号に基づいて、再生側からのオーディオデータの記録を制御することにより違法なコピーを防止するシステムである。

【0004】具体的にはSCMS信号は、オーディオデータが、何度でもコピーが許容されるコピーフリー（copy free）のデータであるか、1度だけコピーが許されている（copy once allowed）データであるか、またはコピーが禁止されている（copy prohibited）データであるかを表す信号である。データ記録側において、D I

Fからオーディオデータを受信すると、そのオーディオデータとともに送信されるSCMS信号を検出する。そして、SCMS信号が、コピーフリー (copy free) となっている場合には、オーディオデータをSCMS信号とともにミニディスクに記録する。また、SCMS信号が、コピーを1度のみ許可 (copy once allowed) となっている場合には、SCMS信号をコピー禁止 (copy prohibited) に変更して、オーディオデータとともに、ミニディスクに記録する。さらに、SCMS信号が、コピー禁止 (copy prohibited) となっている場合には、オーディオデータの記録を行わない。このようなSCMSを使用した制御を行なうことで、ミニディスク装置では、SCMSによって、著作権を有するオーディオデータが、違法にコピーされるのを防止するようになっている。

【0005】しかしながら、SCMSによる制御を行なうためには、データを記録する機器自身がSCMS信号に基づいて、再生側からのオーディオデータの記録制御を実行する構成を有していることが前提となる。従って、SCMS制御を行なう構成を持たない機器での対処は困難となる。そこで、例えば、DVDプレーヤでは、コンテンツ・スクランブルシステムを採用することにより、著作権を有するデータの違法コピーを防止する構成となっている。

【0006】コンテンツ・スクランブルシステムでは、DVDプレーヤに装着されるDVD-ROM(Read Only Memory)に、ビデオデータやオーディオデータ等を暗号化して記録し、暗号化されたデータの復号に用いるキー(復号鍵)を、ライセンスを受けたDVDプレーヤに与える。ライセンスは、不正コピーを行わない等の所定の動作規定に従う処理を実行するように設計されたDVDプレーヤに対して与えられる。従って、ライセンスを受けたDVDプレーヤでは、与えられたキーを利用して、DVD-ROMに記録された暗号化データを復号することにより、DVD-ROMから画像や音声を再生することができる。

【0007】一方、ライセンスを受けていないDVDプレーヤは、暗号化されたデータを復号するためのキーを有していないため、DVD-ROMに記録された暗号化データの復号を行うことができない。このように、コンテンツ・スクランブルシステムでは、ライセンス時に要求される条件を満たしていないDVDプレーヤは、デジタルデータを記録したDVD-ROMの再生を行なえないことになり、不正コピーが防止されるようになっている。

【0008】しかしながら、DVD-ROMで採用されているコンテンツ・スクランブルシステムは、ユーザによるデータの書き込みが不可能な記録媒体(以下、適宜、ROMメディアという)を対象としており、ユーザによるデータの書き込みが可能な記録媒体(以下、適

宜、RAMメディアという)への適用については考慮されていない。

【0009】即ち、ROMメディアに記録されたデータが暗号化されていても、その暗号化されたデータを、そのまま全部、RAMメディアにコピーした場合には、ライセンスを受けた正当な装置で再生可能な、いわゆる海賊版を作成することができてしまう。

【0010】そこで、本出願人は、先の特許出願、特開平11-224461号公報(特願平10-25310号)において、個々の記録媒体を識別する為の情報(以下、媒体識別情報と記述する)を、他のデータとともに記録媒体に記録し、この媒体識別情報のライセンスを受けた装置であることを条件として、その条件が満たされた場合にのみ記録媒体の媒体識別情報へのアクセスが可能となる構成を提案した。

【0011】この方法では、記録媒体上のデータは、媒体識別情報と、ライセンスを受けることにより得られる秘密キー(マスターキー)により暗号化され、ライセンスを受けていない装置が、この暗号化されたデータを読み出したとしても、意味のあるデータを得ることができないようになっている。なお、装置はライセンスを受ける際、不正な複製(違法コピー)ができないように、その動作が規定される。

【0012】ライセンスを受けていない装置は、媒体識別情報にアクセスできず、また、媒体識別情報は個々の媒体毎に個別の値となっているため、ライセンスを受けていない装置が、記録媒体に記録されている、暗号化されたデータのすべてを新たな記録媒体に複製したとしても、そのようにして作成された記録媒体に記録されたデータは、ライセンスを受けていない装置は勿論、ライセンスを受けた装置においても、正しく復号することができないから、実質的に、違法コピーが防止されることになる。

【0013】

【発明が解決しようとする課題】昨今、小型のハードディスクを装着可能な携帯型の記録再生装置としてハードディスクレコーダ(HDR: Hard Disk Recorder)、あるいはフラッシュメモリを搭載した記録再生装置など、様々な記憶媒体をコンテンツ格納媒体として用いた記録再生装置が利用されている。このような状況下において、複数の情報記録再生装置、例えば、DVD-RAMを搭載したDVR(Digital Versatile Recorder)システムと、ハードディスクを搭載したHDRシステムなどの機器間でコンテンツをコピーさせる処理がごく日常的に行われ、また、インターネット配信、あるいは衛星を介してブロードキャスト配信されるコンテンツをRAMメディアに対して格納するなどの処理も頻繁に行なわれるようになってきている。

【0014】このような場合、コンテンツはライセンス

を受けた機器においてのみ利用可能とする構成とすることが原則であり、各ライセンス機器独自の暗号処理用の鍵を用いて各記録媒体にコンテンツを記録する処理が行われる。従って、他の機器、あるいはコンテンツ配信サーバから入力するコンテンツは暗号化されていないデータを入力した場合は、各ライセンス機器独自の暗号処理用の鍵を用いて暗号化した後に記録媒体に記録し、また、入力データが暗号化されている場合には、その暗号化データを復号した後、各ライセンス機器独自の暗号処理用の鍵を用いて再暗号化して記録媒体に記録するという処理を実行することになる。例えば、DVRシステムでは、述した媒体識別情報と、ライセンスを受けることにより得られる秘密キー（マスターキー）などを適用して暗号処理用の鍵を生成してコンテンツ暗号化を行なうことになる。

【0015】しかしながら、このようなコンテンツのコピー処理、あるいは格納時に入力データの復号、再暗号化処理を実行することは、処理速度の低下を招くことになる。本発明は、このような機器間の暗号化データ移動、複製処理、あるいはデータ配信サイトから提供される暗号化データの格納において、データの復号、再暗号化処理を省略し、かつ格納データの復号を正当なライセンスを受けた機器においてのみ実行可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とする。

【0016】

【課題を解決するための手段】本発明の第1の側面は、情報の暗号処理を実行する暗号処理手段を有する情報処理装置であり、前記暗号処理手段は、予め設定された暗号処理シーケンスに従って鍵を生成し、生成した鍵を適用して記録媒体に格納された暗号データの復号処理を実行する構成を有するとともに、記録媒体格納処理対象データとして外部から入力する入力暗号データに対応して設定された第1暗号鍵に対して、前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理を実行して第2暗号鍵を生成する処理を実行し、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行により前記入力暗号データの復号用鍵を生成する処理を実行する構成を有することを特徴とする情報処理装置にある。

【0017】さらに、本発明の情報処理装置の一実施態様において、前記暗号処理シーケンスは、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかを適用した暗号処理として実行される暗号処理シーケンスであり、前記入力暗号データの復号用鍵の生成においては、前記第2暗号鍵と、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかを適用した暗号処理シーケンスを実行する構成であることを特徴とする。

【0018】さらに、本発明の情報処理装置の一実施態

様において、前記第1暗号鍵は、外部から入力する前記入力暗号データとしてのコンテンツに対して設定されるタイトル固有キーであり、前記第2暗号鍵は、前記タイトル固有キーの復号処理により取得可能なタイトルキーであり、前記入力暗号データの復号用鍵は、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかの鍵と、前記タイトルキーとの双方を適用した暗号処理により生成される鍵であることを特徴とする。

【0019】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを格納し、前記暗号処理手段は、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（EKB）の復号処理を実行し、該複合処理によって取得可能な鍵と、前記第2暗号鍵とを適用して前記前記暗号処理シーケンスを実行して前記入力暗号データの復号用鍵を生成する処理を実行する構成を有することを特徴とする。

【0020】さらに、本発明の情報処理装置の一実施態様において、前記入力暗号データは、トランスポートストリームを構成するパケットからなるブロックデータとして入力され、前記暗号処理手段は、前記第2暗号鍵を適用して、前記復号用鍵としての各ブロックデータに対応するブロックキーの生成処理を実行する構成であることを特徴とする。

【0021】さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、前記前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理による前記第2暗号鍵の生成処理、または、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行において、適用鍵の鍵長を変更する縮合処理または伸長処理を実行する構成であることを特徴とする。

【0022】さらに、本発明の情報処理装置の一実施態様において、前記暗号処理手段は、外部から入力する入力暗号データの入力処理に際して、データ送信装置との認証処理を実行し、認証の成立を条件として、入力暗号データの入力処理を実行する構成であることを特徴とする。

【0023】さらに、本発明の情報処理装置の一実施態様において、前記情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを格納し、前記暗号処理手段は、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キーブロック（EKB）の復号処理を実行し、該複合処理によって前記第1暗号鍵の取得処理を実行する構成であることを特徴とする。

【0024】さらに、本発明の第2の側面は、情報の暗号処理を実行する情報処理方法であり、予め設定された暗号処理シーケンスに従って鍵を生成し、生成した鍵を適用して記録媒体に格納された暗号データの復号処理を実行するステップと、記録媒体格納処理対象データとして外部から入力する入力暗号データに対応して設定された第1暗号鍵に対して、前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理を実行して第2暗号鍵を生成するステップと、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行により前記入力暗号データの復号用鍵を生成する処理を実行するステップと、を有することを特徴とする情報処理方法にある。

【0025】さらに、本発明の情報処理方法の一実施態様において、前記暗号処理シーケンスは、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかを適用した暗号処理として実行される暗号処理シーケンスであり、前記入力暗号データの復号用鍵の生成においては、前記第2暗号鍵と、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかを適用した暗号処理シーケンスを実行することを特徴とする。

【0026】さらに、本発明の情報処理方法の一実施態様において、前記第1暗号鍵は、外部から入力する前記入力暗号データとしてのコンテンツに対して設定されるタイトル固有キーであり、前記第2暗号鍵は、前記タイトル固有キーの復号処理により取得可能なタイトルキーであり、前記入力暗号データの復号用鍵は、情報処理装置の格納鍵、または記録媒体の格納鍵の少なくともいずれかの鍵と、前記タイトルキーとの双方を適用した暗号処理により生成される鍵であることを特徴とする。

【0027】さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法を実行する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを有し、前記入力暗号データの復号用鍵を生成するステップにおいて、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キープロック(EKB)の復号処理を実行し、該複合処理によって取得可能な鍵と、前記第2暗号鍵とを適用して前記前記暗号処理シーケンスを実行して前記復号用鍵を生成する処理を実行することを特徴とする。

【0028】さらに、本発明の情報処理方法の一実施態様において、前記入力暗号データは、トランスポートストリームを構成するパケットからなるブロックデータとして入力され、前記第2暗号鍵を適用して、前記復号用鍵としての各ブロックデータに対応するブロックキーの生成処理を実行することを特徴とする。

【0029】さらに、本発明の情報処理方法の一実施態様において、前記前記暗号処理シーケンスの少なくとも

一部シーケンスを逆方向処理とした復号処理による前記第2暗号鍵の生成処理、または、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行において、適用鍵の鍵長を変更する縮合処理または伸長処理を実行することを特徴とする。

【0030】さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法において、さらに、外部から入力する入力暗号データの入力処理に際して、データ送信装置との認証処理を実行し、認証の成立を条件として、入力暗号データの入力処理を実行することを特徴とする。

【0031】さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法を実行する情報処理装置は、複数の異なる情報処理装置をリーフとした階層ツリー構造を構成する各ノードに固有のノードキーと各情報処理装置固有のリーフキーとを有し、ノードキーを下位階層のノードキーまたはリーフキーの少なくともいずれかを含むキーにより暗号化した有効化キープロック(EKB)の復号処理を実行し、該複合処理によって前記第1暗号鍵の取得処理を実行することを特徴とする。

【0032】さらに、本発明の第3の側面は、情報の暗号処理をコンピュータ・システム上で実行せしめるコンピュータ・プログラムであって、予め設定された暗号処理シーケンスに従って鍵を生成し、生成した鍵を適用して記録媒体に格納された暗号データの復号処理を実行するステップと、記録媒体格納処理対象データとして外部から入力する入力暗号データに対応して設定された第1暗号鍵に対して、前記暗号処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理を実行して第2暗号鍵を生成するステップと、前記第2暗号鍵を適用した前記暗号処理シーケンスの実行により前記入力暗号データの復号用鍵を生成する処理を実行するステップと、を具備することを特徴とするコンピュータ・プログラムにある。

【0033】なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能なコンピュータ・システムに対して、コンピュータ可読形式で提供する記憶媒体、通信媒体、例えば、CDやFD、MOなどの記録媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【0034】本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【0035】

【発明の実施の形態】以下、本発明の構成について図面を参照して詳細に説明する。なお、説明手順は、以下の項目に従って行なう。

1. 情報処理装置の構成および処理概要
2. 記録媒体上のコンテンツフォーマット
3. キー配信構成としてのツリー（木）構造について
4. マスターキーを用いた暗号処理によるコンテンツの記録再生
5. メディアキーを用いた暗号処理によるコンテンツの記録再生
6. LSIキーを用いた暗号処理によるコンテンツの記録再生
7. コピー制御
8. 再暗号化を不要としたコンテンツコピーまたは格納処理

8. 1. 機器間のコンテンツコピー処理
8. 2. 配信コンテンツの格納処理
9. 情報処理装置、サーバの構成

【0036】[1. 情報処理装置の構成および処理概要] 図1は、本発明の情報処理装置としての記録再生装置100の一実施例構成を示すブロック図である。記録再生装置100は、例えば、データ記録再生可能なRAMディスクを装着し、RAMディスクに対するデータの読書きを実行するDVRシステム、あるいはデータ記録再生可能なハードディスクを装着し、ハードディスクに対するデータの読書きを実行するHDRシステムなどであり、DVD、CD等の光ディスク、光磁気ディスク、HD等の磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体に対するデータの記録再生を実行する装置である。

【0037】記録再生装置100は、入出力I/F (Interface) 120、MPEG (Moving Picture Experts Group) コーデック130、A/D、D/Aコンバータ141を備えた入出力I/F (Interface) 140、暗号処理手段150、ROM (Read Only Memory) 160、CPU (Central Processing Unit) 170、メモリ180、記録媒体195のドライブ190、さらにトランスポート・ストリーム処理手段 (TS処理手段) 300を有し、これらはバス110によって相互に接続されている。

【0038】入出力I/F 120は、外部から供給される画像、音声、プログラム等の各種コンテンツを構成するデジタル信号を受信し、バス110上に出力するとともに、バス110上のデジタル信号を受信し、外部に出力する。MPEGコーデック130は、バス110を介して供給されるMPEG符号化されたデータを、MPEGデコードし、入出力I/F 140に出力するとともに、入出力I/F 140から供給されるデジタル信号をMPEGエンコードしてバス110上に出力する。入出力I/F 140は、A/D、D/Aコンバータ14

1を内蔵している。入出力I/F 140は、外部から供給されるコンテンツとしてのアナログ信号を受信し、A/D、D/Aコンバータ141でA/D (Analog Digital) 変換することで、デジタル信号として、MPEGコーデック130に出力するとともに、MPEGコーデック130からのデジタル信号を、A/D、D/Aコンバータ141でD/A (Digital Analog) 変換することで、アナログ信号として、外部に出力する。

【0039】暗号処理手段150は、例えば、1チップのLSI (Large Scale Integrated Circuit) で構成され、バス110を介して供給されるコンテンツとしてのデジタル信号を暗号化し、または復号し、バス110上に出力する構成を持つ。なお、暗号処理手段150は1チップLSIに限らず、各種のソフトウェアまたはハードウェアを組み合わせた構成によって実現することも可能である。ソフトウェア構成による処理手段としての構成については後段で説明する。

【0040】ROM 160は、例えば、記録再生装置ごとに固有の、あるいは複数の記録再生装置のグループごとに固有のデバイスキーであるリーフキーと、複数の記録再生装置、あるいは複数のグループに共有のデバイスキーであるノードキーを記憶している。CPU 170は、メモリ180に記憶されたプログラムを実行することで、MPEGコーデック130や暗号処理手段150等を制御する。メモリ180は、例えば、不揮発性メモリで、CPU 170が実行するプログラムや、CPU 170の動作上必要なデータを記憶する。ドライブ190は、デジタルデータを記録再生可能な記録媒体195を駆動することにより、記録媒体195からデジタルデータを読み出し (再生し)、バス110上に出力するとともに、バス110を介して供給されるデジタルデータを、記録媒体195に供給して記録させる。また、プログラムをROM 160に、デバイスキーをメモリ180に記憶するようにしてもよい。

【0041】記録媒体195は、例えば、DVD、CD等の光ディスク、光磁気ディスク、HD等の磁気ディスク、磁気テープ、あるいはRAM等の半導体メモリ等のデジタルデータの記憶可能な媒体であり、本実施の形態では、ドライブ190に対して着脱可能な構成であるとする。但し、記録媒体195は、記録再生装置100に内蔵する構成としてもよい。

【0042】トランスポート・ストリーム処理手段 (TS処理手段) 300は、後段において図6以下を用いて詳細に説明するが、例えば複数のTVプログラム (コンテンツ) が多重化されたトランスポートストリームから特定のプログラム (コンテンツ) に対応するトランスポートパケットを取り出して、取り出したトランスポートストリームの出現タイミング情報を各パケットとともに記録媒体195に格納するためのデータ処理および、記録媒体195からの再生処理時の出現タイミング制御処

理を行なう。

【0043】トランスポートストリームには、各トランスポートパケットの出現タイミング情報としてのATS (Arrival Time Stamp: 着信時刻スタンプ) が設定されており、このタイミングはMPEG2システムズで規定されている仮想的なデコーダであるTSTD (Transport stream System Target Decoder)を破綻させないように符号化時に決定され、トランスポートストリームの再生時には、各トランスポートパケットに付加されたATSによって出現タイミングを制御する。トランスポート・ストリーム処理手段(TS処理手段)300は、これらの制御を実行する。例えば、トランスポートパケットを記録媒体に記録する場合には、各パケットの間隔を詰めたソースパケットとして記録するが、各トランスポートパケットの出現タイミングを併せて記録媒体に保存することにより、再生時に各パケットの出力タイミングを制御することが可能となる。トランスポート・ストリーム処理手段(TS処理手段)300は、DVD等の記録媒体195へのデータ記録時に、各トランスポートパケットの入力タイミングを表すATS (Arrival Time Stamp: 着信時刻スタンプ) を付加して記録する。

【0044】本発明の記録再生装置100は、上述のATSの付加されたトランスポートストリームによって構成されるコンテンツについて、暗号処理手段150において暗号化処理を実行し、暗号化処理のなされたコンテンツを記録媒体195に格納する。さらに、暗号処理手段150は、記録媒体195に格納された暗号化コンテンツの復号処理を実行する。これらの処理の詳細については、後段で説明する。

【0045】記録媒体195には、例えばディスクの製造時のスタンパー毎に設定されるスタンパーID、ディスク毎に異なって設定されるディスクID、コンテンツ毎に異なって設定するコンテンツID、あるいは暗号処理用のキー等、様々な識別データ、暗号処理鍵等が格納される。

【0046】記録媒体195に格納された秘密情報は暗号処理手段150において復号され、復号した秘密情報を用いて記録媒体に対するコンテンツ記録、再生時に適用する暗号処理鍵を生成する。秘密情報は暗号処理手段150内で実行されるコンテンツ暗号化キー生成においてのみ使用される構成であり、秘密情報の外部への漏洩を防止した構成となっている。

【0047】なお、図1に示す暗号処理手段150、TS処理手段300は、理解を容易にするため、別ブロックとして示してあるが、各機能を実行する1つまたは複数のLSIとして構成してもよく、また、各機能のいずれかをソフトウェアまたはハードウェアを組み合わせた構成によって実現する構成としてもよい。

【0048】本発明の記録再生装置の構成例としては図1に示す構成の他に図2に示す構成が可能である。図2

に示す記録再生装置200では、記録媒体205はドライブ装置としての記録媒体インタフェース(I/F)210から着脱が可能であり、この記録媒体205を別の記録再生装置に装着してもデータの読出し、書きこみが可能な構成としたものである。

【0049】次に、図1あるいは図2の記録再生装置における記録媒体に対するデータ記録処理および記録媒体からのデータ再生処理について、図3および図4のフローチャートを参照して説明する。外部からのデジタル信号のコンテンツを、記録媒体195に記録する場合においては、図3(A)のフローチャートにしたがった記録処理が行われる。即ち、デジタル信号のコンテンツ(デジタルコンテンツ)が、例えば、IEEE(Institute of Electrical and Electronics Engineers)1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS301において、入出力I/F120は、供給されるデジタルコンテンツを受信し、バス110を介して、TS処理手段300に出力する。

【0050】TS処理手段300は、ステップS302において、トランスポートストリームを構成する各トランスポートパケットにATSを付加したブロックデータを生成して、バス110を介して、暗号処理手段150に出力する。

【0051】暗号処理手段150は、ステップS303において、受信したデジタルコンテンツに対する暗号化処理を実行し、その結果得られる暗号化コンテンツを、バス110を介して、ドライブ190、あるいは記録媒体I/F210に出力する。暗号化コンテンツは、ドライブ190、あるいは記録媒体I/F210を介して記録媒体195に記録(S304)され、記録処理を終了する。なお、暗号処理手段150における暗号処理については後段で説明する。

【0052】なお、IEEE1394シリアルバスを介して接続した装置相互間で、デジタルコンテンツを伝送するときの、デジタルコンテンツを保護するための規格として、本特許出願人であるソニー株式会社を含む5社によって、5CDTCP(Five Company Digital Transmission Content Protection) (以下、適宜、DTCPという)が定められているが、このDTCPでは、コピーフリーでないデジタルコンテンツを装置相互間で伝送する場合、データ伝送に先立って、送信側と受信側が、コピーを制御するためのコピー制御情報を正しく取り扱うかどうかの認証を相互に行い、その後、送信側において、デジタルコンテンツを暗号化して伝送し、受信側において、その暗号化されたデジタルコンテンツ(暗号化コンテンツ)を復号するようになっている。

【0053】このDTCPに規格に基づくデータ送受信においては、データ受信側の入出力I/F120は、ステップS301で、IEEE1394シリアルバスを介して暗号化コンテンツを受信し、その暗号化コンテンツを、DT

CPに規格に準拠して復号し、平文のコンテンツとして、その後、暗号処理手段150に出力する。

【0054】DTCPによるデジタルコンテンツの暗号化は、時間変化するキーを生成し、そのキーを用いて行われる。暗号化されたデジタルコンテンツは、その暗号化に用いたキーを含めて、IEEE1394シリアルバス上を伝送され、受信側では、暗号化されたデジタルコンテンツを、そこに含まれるキーを用いて復号する。

【0055】なお、DTCPによれば、正確には、キーの初期値と、デジタルコンテンツの暗号化に用いるキーの変更タイミングを表すフラグとが、暗号化コンテンツに含まれる。そして、受信側では、その暗号化コンテンツに含まれるキーの初期値を、やはり、その暗号化コンテンツに含まれるフラグのタイミングで変更していくことで、暗号化に用いられたキーが生成され、暗号化コンテンツが復号される。但し、ここでは、暗号化コンテンツに、その復号を行うためのキーが含まれていると等価であると考えても差し支えないため、以下では、そのように考えるものとする。ここで、DTCPについては、例えば、<http://www.dtcp.com>のURL(Uniform Resource Locator)で特定されるWebページにおいて、インフォメーションバージョン(Informational Version)の取得が可能である。

【0056】次に、外部からのアナログ信号のコンテンツを、記録媒体195に記録する場合の処理について、図3(B)のフローチャートに従って説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS321において、そのアナログコンテンツを受信し、ステップS322に進み、内蔵するA/D、D/Aコンバータ141でA/D変換して、デジタル信号のコンテンツ(デジタルコンテンツ)とする。

【0057】このデジタルコンテンツは、MPEGコーデック130に供給され、ステップS323において、MPEGエンコード、すなわちMPEG圧縮による符号化処理が実行され、バス110を介して、暗号処理手段150に供給される。

【0058】以下、ステップS324、S325、S326において、図3(A)のステップS302、S303における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0059】次に、記録媒体195に記録されたコンテンツを再生して、デジタルコンテンツ、あるいはアナログコンテンツとして出力する処理について図4のフローに従って説明する。デジタルコンテンツとして外部に出力する処理は図4(A)のフローチャートにしたがった再生処理として実行される。即ち、まず最初に、ス

テップS401において、ドライブ190または記録媒体I/F210によって、記録媒体195に記録された暗号化コンテンツが読み出され、バス110を介して、暗号処理手段150に出力される。

【0060】暗号処理手段150では、ステップS402において、ドライブ190または記録媒体I/F210から供給される暗号化コンテンツが復号処理され、復号データがバス110を介して、TS処理手段300に出力される。

【0061】TS処理手段300は、ステップS403において、トランスポートストリームを構成する各トランスポートパケットのATSから出力タイミングを判定し、ATSに応じた制御を実行して、バス110を介して、入出力I/F120に供給する。入出力I/F120は、TS処理手段300からのデジタルコンテンツを、外部に出力し、再生処理を終了する。なお、TS処理手段300の処理、暗号処理手段150におけるデジタルコンテンツの復号処理については後述する。

【0062】なお、入出力I/F120は、ステップS404で、IEEE1394シリアルバスを介してデジタルコンテンツを出力する場合には、DTCPの規格に準拠して、上述したように、相手の装置との間で認証を相互に行い、その後、デジタルコンテンツを暗号化して伝送する。

【0063】記録媒体195に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図4(B)のフローチャートに従った再生処理が行われる。

【0064】即ち、ステップS421、S422、S423において、図4(A)のステップS401、S402、S403における場合とそれぞれ同様の処理が行われ、これにより、暗号処理手段150において得られた復号されたデジタルコンテンツは、バス110を介して、MPEGコーデック130に供給される。

【0065】MPEGコーデック130では、ステップS424において、デジタルコンテンツがMPEGデコード、すなわち伸長処理が実行され、入出力I/F140に供給される。入出力I/F140は、ステップS424において、MPEGコーデック130でMPEGデコードされたデジタルコンテンツを、内蔵するA/D、D/Aコンバータ141でD/A変換(S425)して、アナログコンテンツとする。そして、ステップS426に進み、入出力I/F140は、そのアナログコンテンツを、外部に出力し、再生処理を終了する。

【0066】[2. 記録媒体上のコンテンツフォーマット] 次に、図5を用いて、本発明における記録媒体上のデータフォーマットを説明する。ここで説明するデータフォーマットは、例えばDVRシステムにおいてメディアに格納されるデータ・フォーマットである。以下、記録媒体上のデータの読み書きの最小単位をブロック(block)

ck)という名前と呼ぶ。1ブロックは、 $192 \times X$ (エックス) バイト (例えば $X=32$) の大きさとなっている。

【0067】本発明では、MPEG2のTS (トランスポート・ストリーム) パケット (188バイト) にATSを付加して192バイトとして、それをX個集めて1ブロックのデータとしている。ATSは24乃至32ビットの着信時刻を示すデータであり、先にも説明したようにArrival Time Stamp (着信時刻スタンプ) の略である。ATSは各パケットの着信時刻に応じたランダム性のあるデータとして構成される。記録媒体のひとつのブロック (セクタ) には、ATSを付加したTS (トランスポート・ストリーム) パケットをX個記録する。本発明の構成では、トランスポートストリームを構成する各ブロックの第1番目のTSパケットに付加されたATSを用いてそのブロック (セクタ) のデータを暗号化するブロックキーを生成する。

【0068】ランダム性のあるATSを用いて暗号化用のブロックキーを生成することにより、ブロック毎に異なる固有キーが生成される。生成されたブロック固有キーを用いてブロック毎の暗号化処理を実行する。また、ATSを用いてブロックキーを生成する構成とすることにより、各ブロック毎の暗号化鍵を格納するための記録媒体上の領域が不要となり、メインデータ領域が有効に使用可能となる。さらに、データの記録、再生時にメインデータ部以外のデータをアクセスする必要もなくなり、処理が効率的になる。

【0069】なお、図5に示すブロック・シード (Block Seed) は、ATSを含む付加情報である。ブロック・シードは、さらにATSだけでなくコピー制御情報 (CCI: Copy Control Information) も付加した構成としてもよい。この場合、ATSとCCIを用いてブロックキーを生成する構成とすることができる。

【0070】なお、ここで、ブロック・シードに含まれるコピー制限情報 (CCI: Copy Control Information) は、後段で説明するが、企業5社の共同提案としての5CDTCP (Digital Transmission Content Protection) システムで提唱するコピー制御情報 (CCI: Copy Control Information) であり、デバイスの能力に応じた2種類の情報、すなわち、EMI (Encryption Mode Indicator)、あるいは、コピー制御情報を送るための場所があらかじめ確保されているようなフォーマットにおいて適用されるコンテンツに埋め込まれたコピー制御情報 (CCI) である埋め込みCCI (Embedded CCI) のいずれかの情報を反映したものとなる。

【0071】なお、本発明の構成においては、DVD等の記録媒体上にデータを格納する場合、コンテンツの大部分のデータは暗号化されるが、図5の最下段に示すように、ブロックの先頭のm (たとえば、 $m=8$ または16) バイトは暗号化されずに平文 (Unencrypted data)

のまま記録され、残りのデータ ($m+1$ バイト以降) が暗号化される。これは暗号処理が8バイト単位としての処理であるために暗号処理データ長 (Encrypted data) に制約が発生するためである。なお、もし、暗号処理が8バイト単位でなく、たとえば1バイト単位で行なえるなら、 $m=4$ として、ブロックシード以外の部分をすべて暗号化してもよい。

【0072】ここで、ATSの機能について詳細に説明する。ATSは、先にも説明したように入力トランスポートストリーム中の各トランスポートパケットの出現タイミングを保存するために付加する着信時刻スタンプである。

【0073】すなわち、例えば複数のTVプログラム (コンテンツ) が多重化されたトランスポートストリームの中から1つまたは幾つかのTVプログラム (コンテンツ) を取り出した時、その取り出したトランスポートストリームを構成するトランスポートパケットは、不規則な間隔で現れる (図7(a) 参照)。トランスポートストリームは、各トランスポートパケットの出現タイミングに重要な意味があり、このタイミングはMPEG2システムズ (ISO/IEC 13818-1) で規定されている仮想的なデコーダであるTSTD (Transport stream System Target Decoder) を破綻させないように符号化時に決定される。

【0074】トランスポートストリームの再生時には、各トランスポートパケットに付加されたATSによって出現タイミングが制御される。従って、記録媒体にトランスポートパケットを記録する場合には、トランスポートパケットの入力タイミングを保存する必要があり、トランスポートパケットをDVD等の記録媒体に記録する時に、各トランスポートパケットの入力タイミングを表すATSを付加して記録する。

【0075】図6に、ディジタルインタフェース経由で入力されるトランスポートストリームをDVD等の記録媒体であるストレージメディアに記録する時のTS処理手段300において実行する処理を説明するブロック図を示す。端子600からは、ディジタル放送等のディジタルデータとしてトランスポートストリームが入力される。図1または図2においては、入出力I/F120を介して、あるいは入出力I/F140、MPEGコーデック130を介して端子600からトランスポートストリームが入力される。

【0076】トランスポートストリームは、ビットストリームパーサー (parser) 602に入力される。ビットストリームパーサー602は、入力トランスポートストリームの中からPCR (Program Clock Reference) パケットを検出する。ここで、PCRパケットとは、MPEG2システムズで規定されているPCRが符号化されているパケットである。PCRパケットは、100msec以内の時間間隔で符号化されている。PCRは、ラン

スポーツ packets が受信側に到着する時刻を 27MHz の精度で表す。

【0077】そして、27MHz PLL 603 において、記録再生器が持つ 27MHz クロックをトランスポートストリームの PCR にロック (Lock) させる。タイムスタンプ発生回路 604 は、27MHz クロックのクロックのカウント値に基づいたタイムスタンプを発生する。そして、ブロック・シード (Block seed) 付加回路 605 は、トランスポート packets の第 1 バイト目がスムージングバッファ 606 へ入力される時のタイムスタンプを ATS として、そのトランスポート packets に付加する。

【0078】ATS が付加されたトランスポート packets は、スムージングバッファ 606 を通って、端子 607 から、暗号処理手段 150 に出力され、後段で説明する暗号処理が実行された後、ドライブ 190 (図 1)、記録媒体 I/F 210 (図 2) を介してストレージメディアである記録媒体 195 に記録される。

【0079】図 7 は、入力トランスポートストリームが記録媒体に記録される時の処理の例を示す。図 7 (a) は、ある特定プログラム (コンテンツ) を構成するトランスポート packets の入力を示す。ここで横軸は、ストリーム上の時刻を示す時間軸である。この例ではトランスポート packets の入力は、図 7 (a) に示すように不規則なタイミングで現れる。

【0080】図 7 (b) は、ブロック・シード (Block Seed) 付加回路 605 の出力を示す。ブロック・シード (Block Seed) 付加回路 605 は、トランスポート packets 毎に、その packets のストリーム上の時刻を示す ATS を含むブロック・シード (Block Seed) を付加して、ソース packets を出力する。図 7 (c) は記録媒体に記録されたソース packets を示す。ソース packets は、図 7 (c) に示すように間隔を詰めて記録媒体に記録される。このように間隔を詰めて記録することにより記録媒体の記録領域を有効に使用できる。

【0081】図 8 は、記録媒体 195 に記録されたトランスポートストリームを再生する場合の TS 処理手段 300 の処理構成ブロック図を示している。端子 800 からは、後段で説明する暗号処理手段において復号された ATS 付きのトランスポート packets が、ブロック・シード (Block seed) 分離回路 801 へ入力され、ATS とトランスポート packets が分離される。タイミング発生回路 804 は、再生器が持つ 27MHz クロック 805 のクロックカウンタ値に基づいた時間を計算する。

【0082】なお、再生の開始時において、一番最初の ATS が初期値として、タイミング発生回路 804 にセットされる。比較器 803 は、ATS とタイミング発生回路 804 から入力される現在の時刻を比較する。そして、タイミング発生回路 804 が発生する時間と ATS が等しくなった時、出力制御回路 802 は、そのラン

スポーツ packets を MPEG コーデック 130 またはデジタル出力 I/F 120 へ出力する。

【0083】図 9 は、入力 AV 信号を記録再生器 100 の MPEG コーデック 130 において MPEG エンコードして、さらに TS 処理手段 300 においてトランスポートストリームを符号化する構成を示す。従って図 9 は、図 1 または、図 2 おける MPEG コーデック 130 と TS 処理手段 300 の両処理構成を併せて示すブロック図である。端子 901 からは、ビデオ信号が入力されており、それは MPEG ビデオエンコーダ 902 へ入力される。

【0084】MPEG ビデオエンコーダ 902 は、入力ビデオ信号を MPEG ビデオストリームに符号化し、それをバッファビデオストリームバッファ 903 へ出力する。また、MPEG ビデオエンコーダ 902 は、MPEG ビデオストリームについてのアクセスユニット情報を多重化スケジューラ 908 へ出力する。ビデオストリームのアクセスユニットとは、ピクチャであり、アクセスユニット情報とは、各ピクチャのピクチャタイプ、符号化ビット量、デコードタイムスタンプである。ここで、ピクチャタイプは、I/P/B ピクチャ (picture) の情報である。また、デコードタイムスタンプは、MPEG 2 システムズで規定されている情報である。

【0085】端子 904 からは、オーディオ信号が入力されており、それは MPEG オーディオエンコーダ 905 へ入力される。MPEG オーディオエンコーダ 905 は、入力オーディオ信号を MPEG オーディオストリームに符号化し、それをバッファ 906 へ出力する。また、MPEG オーディオエンコーダ 905 は、MPEG オーディオストリームについてのアクセスユニット情報を多重化スケジューラ 908 へ出力する。オーディオストリームのアクセスユニットとは、オーディオフレームであり、アクセスユニット情報とは、各オーディオフレームの符号化ビット量、デコードタイムスタンプである。

【0086】多重化スケジューラ 908 には、ビデオとオーディオのアクセスユニット情報が入力される。多重化スケジューラ 908 は、アクセスユニット情報に基づいて、ビデオストリームとオーディオストリームをトランスポート packets に符号化する方法を制御する。多重化スケジューラ 908 は、内部に 27MHz 精度の基準時刻を発生するクロックを持ち、そして、MPEG 2 で規定されている仮想的なデコーダモデルである T-ST D を満たすようにして、トランスポート packets の packets 符号化制御情報を決定する。packets 符号化制御情報は、packets 化するストリームの種類とストリームの長さである。

【0087】packets 符号化制御情報がビデオ packets の場合、スイッチ 976 は a 側になり、ビデオストリームバッファ 903 から packets 符号化制御情報により指

示されたペイロードデータ長のビデオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0088】パケット符号化制御情報がオーディオパケットの場合、スイッチ976はb側になり、オーディオストリームバッファ906から指示されたペイロードデータ長のオーディオデータが読み出され、トランスポートパケット符号化器909へ入力される。

【0089】パケット符号化制御情報がPCRパケットの場合、トランスポートパケット符号化器909は、多重化スケジューラ908から入力されるPCRを取り込み、PCRパケットを出力する。パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケット符号化器909へは何も入力されない。

【0090】トランスポートパケット符号化器909は、パケット符号化制御情報がパケットを符号化しないことを指示する場合、トランスポートパケットを出力しない。それ以外の場合、パケット符号化制御情報に基づいてトランスポートパケットを生成し、出力する。したがって、トランスポートパケット符号化器909は、間欠的にトランスポートパケットを出力する。到着 (Arrival) タイムスタンプ (time stamp) 計算手段910は、多重化スケジューラ908から入力されるPCRに基づいて、トランスポートパケットの第1バイト目が受信側に到着する時刻を示すATSを計算する。

【0091】多重化スケジューラ908から入力されるPCRは、MPEG2で規定されるトランスポートパケットの10バイト目の受信側への到着時刻を示すので、ATSの値は、PCRの時刻から10バイト前のバイトが到着する時刻となる。

【0092】ブロック・シード (Block Seed) 付加回路911は、トランスポートパケット符号化器909から出力されるトランスポートパケットにATSを付加する。ブロック・シード (Block seed) 付加回路911から出力されるATS付きのトランスポートパケットは、スムージングバッファ912を通して、暗号処理手段150へ入力され、後段で説明する暗号処理が実行された後、ストレージメディアである記録媒体195へ格納される。

【0093】記録媒体195へ格納されるATS付きのトランスポートパケットは、暗号処理手段150で暗号化される前に図7(c)に示すように間隔を詰めた状態で入力され、その後、記録媒体195に格納される。トランスポートパケットが間隔を詰めて記録されても、ATSを参照することによって、そのトランスポートパケットの受信側への入力時刻を制御することができる。

【0094】ところで、ATSの大きさは32ビットに決まっているわけではなく、24ビット乃至31ビットでも構わない。ATSのビット長が長いほど、ATSの

時間カウンタが一周する周期が長くなる。例えば、ATSが27MHz精度のバイナリカウンタである場合、24-bit長のATSが一周する時間は、約0.6秒である。この時間間隔は、一般のトランスポートストリームでは十分な大きさである。なぜなら、トランスポートストリームのパケット間隔は、MPEG2の規定により、最大0.1秒と決められているからである。しかしながら、十分な余裕を見て、ATSを24-bit以上にしても良い。

【0095】このように、ATSのビット長を様々な長さとした場合、ブロックデータの付加データであるブロックシードの構成としていくつかの構成が可能となる。ブロック・シードの構成例を図10に示す。図10の例1は、ATSを32ビット分使用する例である。図10の例2は、ATSを30ビットとし、コピー制御情報 (CCI) を2ビット分使用する例である。コピー制御情報は、それが付加されたデータのコピー制御の状態を表す情報であり、SCMS: Serial Copy Management SystemやCGMS: Copy Generation Management Systemが有名である。これらのコピー制御情報では、その情報が付加されたデータは制限なくコピーが許可されていることを示すコピーフリー (Copy Free)、1世代のみのコピーを許可する1世代コピー許可 (One Generation Copy Allowed)、コピーを認めないコピー禁止 (Copy Prohibited) などの情報が表せる。

【0096】図10に示す例3は、ATSを24ビットとし、CCIを2ビット使用し、さらに他の情報を6ビット使用する例である。他の情報としては、たとえばこのデータがアナログ出力される際に、アナログ映像データのコピー制御機構であるマクロビジョン (Macrovision) のオン/オフ (On/Off) を示す情報など、様々な情報を利用することが可能である。

【0097】[3. キー配信構成としてのツリー (木) 構造について] 次に、図1または図2に示した記録再生装置が、データを記録媒体に記録、もしくは記録媒体から再生する際に必要なマスターキーを、各機器に配布する構成について説明する。図11は、本方式を用いた記録システムにおける記録再生装置の鍵の配布構成を示した図である。図11の最下段に示すナンバ0~15が個々の記録再生装置である。すなわち図11に示す木 (ツリー) 構造の各葉 (リーフ: leaf) がそれぞれの記録再生装置に相当する。

【0098】各デバイス0~15は、製造時 (出荷時) に、あらかじめ定められている初期ツリーにおける、自分のリーフからルートに至るまでのノードに割り当てられた鍵 (ノードキー) および各リーフのリーフキーを自身で格納する。図11の最下段に示すK0000~K1111が各デバイス0~15にそれぞれ割り当てられたリーフキーであり、最上段のKRから、最下段から2番目の節 (ノード) に記載されたキー: KR~K1111を

ノードキーとする。

【0099】図11に示すツリー構成において、例えばデバイス0はリーフキーK0000と、ノードキー：K000、K00、K0、KRを所有する。デバイス5はK0101、K010、K01、K0、KRを所有する。デバイス15は、K1111、K111、K11、K1、KRを所有する。なお、図11のツリーにはデバイスが0～15の16個のみ記載され、ツリー構造も4段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【0100】また、図11のツリー構造に含まれる各記録再生器には、様々な記録媒体、例えばDVD、CD、MD、HD、メモリスティック（商標）等を使用する様々なタイプの記録再生器が含まれている。さらに、様々なアプリケーションサービスが共存することが想定される。このような異なるデバイス、異なるアプリケーションの共存構成の上に図11に示すキー配布構成が適用されている。

【0101】これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を同一の記録媒体を用いるひとつのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、共通に使用するマスターキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツプロバイダ、あるいは決済処理機関等、各デバイスとのデータ送受信を行なう機関は、図11の点線で囲んだ部分、すなわちデバイス0、1、2、3を1つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図11のツリー中に複数存在する。

【0102】なお、ノードキー、リーフキーは、ある1つの鍵管理センタによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センタ、プロバイダ、決済機関等が実行する。

【0103】このツリー構成において、図11から明らかなように、1つのグループに含まれる3つのデバイス0、1、2、3はノードキーとして共通のキーK00、K0、KRを保有する。このノードキー共有構成を利用することにより、例えば共通のマスターキーをデバイス0、1、2、3のみに提供することが可能となる。たと

えば、共通に保有するノードキーK00自体をマスターキーとして設定すれば、新たな鍵送付を実行することなくデバイス0、1、2、3のみが共通のマスターキーの設定が可能である。また、新たなマスターキーKmasterをノードキーK00で暗号化した値Enc(K00, Kmaster)を、ネットワークを介してあるいは記録媒体に格納してデバイス0、1、2、3に配布すれば、デバイス0、1、2、3のみが、それぞれのデバイスにおいて保有する共有ノードキーK00を用いて暗号Enc(K00, Kmaster)を解いてマスターキー：Kmasterを得ることが可能となる。なお、Enc(Ka, Kb)はKbをKaによって暗号化したデータであることを示す。

【0104】また、ある時点tにおいて、デバイス3の所有する鍵：K0011、K001、K00、K0、KRが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス0、1、2、3のグループ）で送受信されるデータを守るために、デバイス3をシステムから切り離す必要がある。そのためには、ノードキー：K001、K00、K0、KRをそれぞれ新たな鍵K(t)001、K(t)00、K(t)0、K(t)Rに更新し、デバイス0、1、2にその更新キーを伝える必要がある。ここで、K(t)aaaは、鍵Kaaaの世代（Generation）：tの更新キーであることを示す。

【0105】更新キーの配布処理について説明する。キーの更新は、例えば、図12(A)に示す有効化キーブロック（EKB：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス0、1、2に供給することによって実行される。

【0106】図12(A)に示す有効化キーブロック（EKB）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成される。図12の例は、図11に示すツリー構造中のデバイス0、1、2において、世代tの更新ノードキーを配布することを目的として形成されたブロックデータである。図11から明らかなように、デバイス0、デバイス1は、更新ノードキーとしてK(t)00、K(t)0、K(t)Rが必要であり、デバイス2は、更新ノードキーとしてK(t)001、K(t)00、K(t)0、K(t)Rが必要である。

【0107】図12(A)のEKBに示されるようにEKBには複数の暗号化キーが含まれる。最下段の暗号化キーは、Enc(K0010, K(t)001)である。これはデバイス2の持つリーフキーK0010によって暗号化された更新ノードキーK(t)001であり、デバイス2は、自身の持つリーフキーによってこの暗号化キーを復号し、K(t)001を得ることができる。また、復号により得たK(t)001を用いて、図12(A)の下から2段目の暗号化キーEnc(K

(t) 001, K(t) 00) を復号可能となり、更新ノードキーK(t) 00を得ることができる。以下順次、図12(A)の上から2段目の暗号化キーEnc(K(t) 00, K(t) 0)を復号し、更新ノードキーK(t) 0、図12(A)の上から1段目の暗号化キーEnc(K(t) 0, K(t) R)を復号しK(t) Rを得る。一方、デバイス0, 1は、ノードキーK000は更新する対象に含まれておらず、更新ノードキーとして必要なのは、K(t) 00、K(t) 0、K(t) Rである。デバイス0, 1は、図12(A)の上から3段目の暗号化キーEnc(K000, K(t) 00)を復号しK(t) 00、を取得し、以下、図12(A)の上から2段目の暗号化キーEnc(K(t) 00, K(t) 0)を復号し、更新ノードキーK(t) 0、図12(A)の上から1段目の暗号化キーEnc(K(t) 0, K(t) R)を復号しK(t) Rを得る。このようにして、デバイス0, 1, 2は更新した鍵K(t) Rを得ることができる。なお、図12(A)のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【0108】図11に示すツリー構造の上位段のノードキー：K0, KRの更新が不要であり、ノードキーK00のみの更新処理が必要である場合には、図12(B)の有効化キーブロック(EKB: Enabling Key Block)を用いることで、更新ノードキーK(t) 00をデバイス0, 1, 2に配布することができる。

【0109】図12(B)に示すEKBは、例えば特定のグループにおいて共有する新たなマスターキーを配布する場合に利用可能である。具体例として、図11に点線で示すグループ内のデバイス0, 1, 2, 3がある記録媒体を用いており、新たな共通のマスターキーK

(t) masterが必要であるとする。このとき、デバイス0, 1, 2, 3の共通のノードキーK00を更新したK(t) 00を用いて新たな共通の更新マスターキー：K(t) masterを暗号化したデータEnc(K(t), K(t) master)を図12(B)に示すEKBとともに配布する。この配布により、デバイス4など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【0110】すなわち、デバイス0, 1, 2はEKBを処理して得たK(t) 00を用いて上記暗号文を復号すれば、t時点でのマスターキーK(t) masterを得ることが可能になる。

【0111】(EKBを使用したマスターキーの配布) 図13に、t時点でのマスターキーK(t) masterを得る処理例として、K(t) 00を用いて新たな共通のマスターキーK(t) masterを暗号化したデータEnc(K(t) 00, K(t) master)と図12(B)に示すEKBとを記録媒体を介して受領したデバイス0の処理を示す。

【0112】図13に示すように、デバイス0は、記録媒体に格納されている世代：t時点のEKBと自分がかじめ格納しているノードキーK000を用いて上述したと同様のEKB処理により、ノードキーK(t) 00を生成する。さらに、復号した更新ノードキーK

(t) 00を用いて更新マスターキーK(t) masterを復号して、後にそれを使用するために自分だけが持つリーフキーK0000で暗号化して格納する。なお、デバイス0が更新マスターキーK(t) masterを安全に自身内に格納できる場合、リーフキーK0000で暗号化する必要はない。

【0113】また、この更新マスターキーの取得処理を図14のフローチャートにより説明する。なお、記録再生装置は出荷時にその時点で最新のマスターキー：K

(c) masterを与えられ、自身のメモリに安全に(具体的にはたとえば、自身のリーフキーで暗号化して)格納しているものとする。

【0114】更新マスターキーK(n) masterとEKBの格納された記録媒体が、記録再生装置にセットされると、まず最初に、ステップS1401において、記録再生装置は、記録媒体から、記録媒体に格納されているマスターキーK(n) masterの時点(世代)番号：n(これを、プレ(pre-recording)記録世代情報(Generation#n)と呼ぶことにする)を読み出す。記録媒体には、予め、マスターキーK(n) masterの時点(世代)番号：nが記憶されている。また、自身が保持している暗号化マスターキーCを読み出し、ステップS1402において、その暗号化マスターキーの世代：cと、プレ記録世代情報Generation#nが表す世代：nとを比較して、その世代の前後を判定する。

【0115】ステップS1402において、プレ記録世代情報Generation#nが表す世代：nの方が、自身のメモリに記憶された暗号化マスターキーCの世代：cよりも後でない(新しくない)と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代：cが、プレ記録世代情報Generation#nが表す世代：nと同一か、または後の場合、ステップS1403乃至S1408をスキップして、マスターキー更新処理を終了する。即ち、この場合、自身のメモリに記憶されたマスターキーK(c) master(暗号化マスターキーC)の更新は行わないので、その更新は行われぬ。

【0116】一方、ステップS1402において、プレ記録世代情報Generation#nが表す世代：nの方が、メモリに記憶された暗号化マスターキーCの世代：cよりも後である(新しい)と判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代nよりも前の世代である場合、ステップS1403に進み、記録再生装置は、記録媒体から、有効化キーブロック(EKB: Enabling Key Block)を読み出す。

【0117】ステップS1404において、記録再生装置は、ステップS1403で読み出したEKBと、自身がメモリに格納しているリーフキー（図11のデバイス0におけるK0000）およびノードキー（図11のデバイス0におけるK000、K00...）を用いて、プレ記録世代情報Generation#n（図13におけるt）時点でのノード00の鍵K（t）00を計算する。

【0118】ステップS1405では、ステップS1404においてK（t）00を得られたか否かを検査する。得られなかった場合は、その時点においてその記録再生装置がツリー構成のグループからリボーク（排除）されていることを示すので、ステップS1406乃至S1408をスキップしてマスターキー更新処理を終了する。

【0119】K（t）00を得られた場合、ステップS1406に進み、記録媒体からEnc（K（t）00、K（t）master）、すなわち、K（t）00を用いてt時点でのマスターキーを暗号化した値を読み出す。そしてステップS1407において、この暗号文をK（t）00を用いて復号してK（t）masterを計算する。

【0120】ステップS1408では、自身のみが持つリーフキー（図11のデバイス0におけるK0000）を用いてK（t）masterを暗号化してメモリに格納する。以上で、マスターキーの更新処理が完了する。

【0121】ところで、マスターキーは、時点（世代）0から昇順に使用されていくが、新しい世代のマスターキーから、古い世代のマスターキーを計算によりシステム内の各機器が求められる構成とすることが望ましい。すなわち、記録再生装置は、一方向性関数fを保持しており、その一方向性関数fに、自身が持つマスターキーを、そのマスターキーの世代と、必要なマスターキーの世代との差に対応する回数だけ適用することにより、調べた世代のマスターキーを作成する。

【0122】具体的には、例えば、記録再生装置に記憶されているマスターキーMKの世代が世代i+1であり、あるデータの再生に必要な（記録時に使用された）マスターキーMKの世代が世代i-1である場合、マスターキーK（i-1）masterは、記録再生装置において、一方向性関数fが2回用いられ、f（f（K（i+1）master））を計算することにより生成される。

【0123】また、記録再生装置に記憶されているマスターキーの世代が世代i+1であり、必要なマスターキーの世代が世代i-2である場合、マスターキーK（i-2）masterは、一方向性関数fを3回用いて、f（f（f（K（i+1）master）））を計算することにより生成される。

【0124】ここで、一方向性関数としては、例えば、ハッシュ(hash)関数を用いることができる。具体的には、例えば、MD5(Message Digest 5)や、SHA-1(Secure Hash Algorithm - 1)等を採用することができ

る。キーを発行するキー発行機関は、これらの一方向性関数を用いて自身の世代より前の世代を生成可能なマスターキーK（0）master、K（1）master、K（2）master・・・、K（N）masterを、あらかじめ求めておく。即ち、まず最初に、第N世代のマスターキーK

（N）masterを設定し、そのマスターキーK（N）masterに、一方向性関数を1回ずつ適用していくことで、それより前の世代のマスターキーK（N-1）master、K（N-2）master、・・・、K（1）master、K（0）masterを順次生成しておく。そして、世代の小さい（前の）マスターキーK（0）masterから順番に使用していく。なお、自身の世代より前の世代のマスターキーを生成するのに用いる一方向性関数は、すべての記録再生装置に設定されているものとする。

【0125】また、一方向性関数としては、例えば、公開鍵暗号技術を採用することも可能である。この場合、キー発行機関は、公開鍵暗号方式の秘密鍵を所有し、その秘密鍵に対する公開鍵を、すべての再生装置に与えておく。そして、キー発行機関は、第0世代のマスターキーK（0）masterを設定し、そのマスターキーK（0）masterから使用していく。即ち、キー発行機関は、第1世代以降のマスターキーK（i）masterが必要になったら、その1世代前のマスターキーK（i-1）masterを、秘密鍵で変換することにより生成して使用する。この場合、キー発行機関は、一方向性関数を用いて、N世代のマスターキーを、あらかじめ生成しておく必要がない。また、この方法によれば、理論上は、無制限の世代のマスターキーを生成することができる。なお、記録再生装置では、ある世代のマスターキーを有していれば、そのマスターキーを、公開鍵で変換することにより、その世代より前の世代のマスターキーを得ることができる。

【0126】[4. マスターキーを用いた暗号処理によるコンテンツの記録再生] 次に、マスターキーを用いた暗号処理によるコンテンツの記録再生処理について説明する。まず、記録再生装置がコンテンツを自身の記録媒体に記録する場合の、記録再生装置の処理について図15のフローチャートを用いて説明する。コンテンツデータは、ある世代のマスターキーにより暗号化されてネットワークあるいは記録媒体を介してコンテンツプロバイタから各記録再生装置に配布される。

【0127】まず最初に、ステップS1501において、記録再生装置は、記録媒体から、プレ記録世代情報Generation#nを読み出す。また、自身のメモリが記憶している暗号化マスターキーCの世代cを取得し、ステップS1502において、その暗号化マスターキーの世代cと、プレ記録世代情報Generation#nが表す世代nとを比較して、その世代の前後を判定する。

【0128】ステップS1502において、メモリに記憶された暗号化マスターキーCの世代cが、プレ記録世

代情報Generation#nが表す世代n以後でないと判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代cが、プレ記録世代情報Generation#nが表す世代nよりも古い世代である場合、ステップS1503をスキップして、すなわち、コンテンツデータの記録処理を行わずに終了する。

【0129】一方、ステップS1502において、自身の記録再生装置内のメモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代n以後であると判定された場合、即ち、メモリに記憶された暗号化マスターキーCの世代が、プレ記録世代情報Generation#nが表す世代nと同一か、またはそれよりも新しい場合、ステップS1503に進み、コンテンツデータの記録処理を行う。

【0130】以下、世代管理のなされたマスターキーによってコンテンツデータの暗号化処理を実行して、自己の記録媒体に格納する処理について説明する。なお、ここでは、先に説明したトランスポートストリームによって構成されるデータを世代管理されたマスターキーを利用したデータに基づいてブロックキーを生成してブロックキーによりコンテンツデータを暗号化して記録媒体に格納する処理について説明する。

【0131】図16、図17の処理ブロック図および図18のフローチャートを用いて説明する。ここでは、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクID(Disc ID)を、データを暗号化する鍵に作用させるようにしている。

【0132】図16、図17の処理ブロック図に従って、暗号処理手段150が実行するデータの暗号化処理の概要について説明する。

【0133】記録再生装置1600は自身のメモリ180(図1、2参照)に格納しているマスターキー1601、データ解析記録方式用キー(コグニザントキー: Cognizant Key)1631もしくはデータ非解析記録方式用キー(ノンコグニザントキー: Non-Cognizant Key)1632を読み出す。データ解析記録方式用キー(Cognizant Key)、データ非解析記録方式用キー(Non-Cognizant Key)については、後述する。

【0134】マスターキー1601は、図14のフローにより記録再生装置のメモリに格納された秘密キーであり、前述のように世代管理がなされており、それぞれに世代番号が対応付けられている。このマスターキーは、複数の記録再生装置に共通なキー、例えば図11に示す点線枠のグループに属するデバイスに共通なキーである。デバイスIDは記録再生装置1600の識別子であり、予め記録再生装置に格納されている例えば製造番号等の識別子である。このデバイスIDは公開されている。データ解析記録方式用キー(Cognizant Key)

1631、データ非解析記録方式用キー(Non-Cognizant Key)1632は、それぞれの記録モードに対応したキーであり、複数の記録再生装置に共通のキーである。これらは予め記録再生装置1600のメモリに格納されている。

【0135】記録再生装置1600は例えば光ディスクである記録媒体1620に識別情報としてのディスクID(Disc ID)1603が既に記録されているかどうかを検査する。記録されていれば、ディスクID(Disc ID)1603を読み出し(図16に相当)、記録されていなければ、暗号処理手段150においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法でディスクID(Disc ID)1701を生成し、ディスクに記録する(図17に相当)。ディスクID(Disc ID)1603はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。

【0136】記録再生装置1600は、次にマスターキーと、特殊な読み取り方法でのみディスクから読み取り可能な秘密情報として記録されたスタンパーID(Stamper ID)1680と、ディスクID1603を用いて、ディスク固有キー(Disc Unique Key)を生成1602する。

【0137】マスターキーと秘密情報としてのスタンパーID(Stamper ID)1680とディスクID1603とを用いディスク固有キー(Disc Unique Key)の具体的な生成方法としては、図19に示すように、ブロック暗号関数を用いたハッシュ関数にマスターキー(Master Key)とスタンパーID(Stamper ID)とディスクID(Disc ID)を入力して得られた結果を用いる例1の方法や、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとスタンパーID(Stamper ID)とディスクID(Disc ID)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー(Disc Unique Key)として使用する例2の方法が適用できる。

【0138】上述したように、スタンパーID(Stamper ID)1680は、あらかじめディスクに記録されている高度な秘密情報であり、その読み出しおよび読み出されたスタンパーID(Stamper ID)を利用したディスク固有キー(Disc Unique Key)の生成などの演算処理は、秘密が保たれるように暗号処理手段内部で実行される。すなわち、ディスクから読み出された秘密情報は暗号処理手段内においてセキュアに保護される。

【0139】このように、本発明の構成においては、正当なデバイスのみが、たとえばLSI内に実装されて高度に保護された暗号鍵の生成を実行する暗号処理部においてセキュアな保護の下にコンテンツ暗号処理用の鍵生成処理を実行する構成であり、不正なコンテンツの再生処理を効果的に防止することが可能となる。

【0140】記録再生装置1600は、次に、記録ごと

の固有鍵であるタイトルキー (Title Key) を暗号処理手段150 (図1, 2, 参照) においてランダムに、もしくはあらかじめ定められた例えば乱数発生等の方法で生成1604し、ディスク1620に記録する。

【0141】さらに、この記録における記録モードがデータ解析記録方式 (Cognizant Mode) かデータ非解析記録方式 (Non-cognizant) かを表すフラグを設定1633し、ディスク1620に記録モード1635を記録する。

【0142】ここで、データ解析記録方式 (Cognizant Mode) およびデータ非解析記録方式 (Non-Cognizant Mode) について説明する。

【0143】コンテンツはそれぞれあらかじめコンテンツ提供者によっていかなる条件で複製が可能かを指定されている。そこで、ネットワーク接続においてもその指定された条件を正しく相手の機器に伝える必要性があり、企業5社の共同提案としての5C D T C P (Digital Transmission Content Protection) システムではコピー制御情報 (C C I : Copy Control Information) という方法を用いて解決している。コピー制御情報 (C C I) はデバイスの能力に応じて2種類の伝達方法が規定されている。

【0144】エンクリプションモード・インディケータ (E M I : Encryption Mode Indicator) はパケットヘッダにあるS y ビットの上位2ビットを使ってコピー制御情報 (C C I) を送るメカニズムであり、受信デバイスが簡単にアクセスする事ができると同時に、この値がコンテンツを暗号化する鍵に作用するため安全に送ることができるようになっている。

【0145】E M I によりそのパケットの暗号化モードを示し、コンテンツ暗号・復号鍵の生成モードを指定する。E M I をIEEE1394パケットヘッダに置くことにより、受信機器は例えばM P E G 転送ストリーム (MPEG transport stream) の中に埋め込まれている埋め込みコピー制御情報 (Embedded C C I) (後述) を取り出すことなく簡単にどのモードでコンテンツが暗号化されているかを知ることができる。

【0146】図20にIEEE1394パケットフォーマットを示す。データフィールド (Data Field) 中には、音楽データ、画像データ等、様々なコンテンツが格納され、コピー制御情報 (C C I) としてのエンクリプション・モード・インディケータ (E M I : Encryption Mode Indicator) はパケットヘッダにあるS y ビットの上位2ビットに設定される。

【0147】E M I の2ビット情報は、設定値に応じてコンテンツの異なる取り扱いを規定する。具体的には、値00は認証も暗号化も必要がなく、コンテンツは自由にコピーが可能なコピーフリー (Copy Free) を示し、値01は一世代コピーの作成が可能なコピー1ジェネレーション (Copy One Generation) を、値10は前述

のCopy One Generation が一度記録された後の、再コピーが禁止されているノーモアコピー (No More Copies) を、値11はコンテンツがリリース時点からコピー禁止であるネバーコピー (Never Copy) を表す。

【0148】D-VHSやハードディスクのような記録されるデータのフォーマットを認識しないようなビットストリームレコーダでも正しく著作物を取り扱えるように、記録時に埋め込みC C I (Embedded C C I) の更新 (e x. Copy One Generationから No More Copies へ) を必要とせず、E M I の更新のみ行えばよい、という記録方法がデータ非解析 (Non-Cognizant) 記録方式である。

【0149】一方、こういったコピー制御情報を送るための場所があらかじめ確保されているようなフォーマット (たとえばDVフォーマット: DV-format) においては、C C I はコンテンツの一部として伝送することができる。このように、コンテンツの一部としてコンテンツに埋め込まれたコピー制御情報 (C C I) を埋め込みC C I (Embedded C C I) と呼ぶ。通常、コンテンツが暗号化されて転送される場合、埋め込みC C I (Embedded C C I) もコンテンツと同様に暗号化されて転送され、埋め込みC C I (Embedded C C I) の故意の変更は困難とされている。

【0150】ここで、前述したE M I の2ビットのコピー制御情報と、埋め込みC C I (Embedded C C I) との双方を持つコンテンツの場合、コンテンツ記録を実行するある記録デバイスは、E M I および埋め込みC C I (Embedded C C I) の双方のコピー制御情報の更新を行なう。しかし、埋め込みC C I (Embedded C C I) の解析能力のない記録デバイスの場合、E M I は更新するが、埋め込みC C I (Embedded C C I) の更新は実行しないことになる。

【0151】コンテンツ記録時に、記録デバイスがコンテンツの一部として伝送された埋め込みC C I (Embedded C C I) の更新を行ってコンテンツとともに記録する記録方式をデータ解析 (Cognizant) 記録方式という。データ解析 (Cognizant) 記録方式と、データ非解析 (Non-Cognizant) 記録方式では、データ非解析 (Non-Cognizant) 記録方式の方が埋め込みC C I (Embedded C C I) の更新を行わなくてよい分、負荷が軽く実装しやすいが、5C D T C P のルールとして、その機器がコンテンツをM P E G デコードしてアナログ端子から映像信号を表示するためにはその機器はデータ解析記録方式 (Cognizant Mode) でなければならないというルールがあり、デコード/表示機能を持つ機器はデータ解析記録方式 (Cognizant Mode) を実行する機能を備えていることが必要である。

【0152】しかしまた、データ解析記録方式 (Cognizant Mode) を実行するためには、コンテンツの一部として埋め込まれている埋め込みC C I (Embedded C C I) の

位置や意味を完全に知る必要があり、たとえばある機器が市場に出た後に制定された新規のあるいは更新されたデータフォーマットについては、その新しいデータフォーマットに対して、古い機器がデータ解析記録方式 (Cognizant Mode) を実行するのは非常に困難となる場合がある。

【0153】従って、コンテンツを記録するある機器が、特定のデータフォーマットについては、もしくは、特定の機能を実現するときには、データ解析記録方式 (Cognizant Mode) を実行し、また異なるデータフォーマットのコンテンツ記録時には、データ非解析記録方式 (Non-Cognizant Mode) を実行するといった、両方の記録方式を実行することが考えられる。

【0154】また、すべてのコンテンツに対して、データ非解析記録方式 (Non-Cognizant Mode) の記録しか行わない機器も存在する。また、逆に埋め込みCCI (Embedded CCI) を理解できるフォーマットを持つコンテンツの処理しか実行しない機器、すなわちデータ解析記録方式 (Cognizant Mode) のみ実行する機器も存在することが考えられる。

【0155】このように、2つのコピー制御情報、すなわちEMIと埋め込みCCI (Embedded CCI) が存在し、またコンテンツ記録を実行する機器としても、データ解析記録方式 (Cognizant Mode) を実行する機器と、データ非解析記録方式 (Non-Cognizant Mode) の記録を実行する機器が混在する状況においては、データ解析記録方式 (Cognizant Mode) で記録したコンテンツと、データ非解析記録方式 (Non-Cognizant Mode) で記録したコンテンツは明確に区別されることが好ましい。

【0156】すなわち、データ解析記録方式 (Cognizant Mode) でコンテンツを記録した場合にはEMIも埋め込みCCI (Embedded CCI) の双方のコピー制御情報が更新されるが、データ非解析記録方式 (Non-Cognizant Mode) でコンテンツの記録が実行された場合は、EMIのみが更新され、埋め込みCCI (Embedded CCI) の更新が行なわれない。その結果、記録媒体上のEMIと埋め込みCCI (Embedded CCI) に不整合がおこり、その両者が混ざると混乱が生じるためである。従って、2つのコピー制御情報の不整合を発生させないためには、データ解析記録方式 (Cognizant Mode) で記録されたコンテンツは、データ解析記録方式 (Cognizant Mode) モードでの記録再生処理を実行し、データ非解析記録方式 (Non-Cognizant Mode) で記録されたコンテンツはデータ非解析記録方式 (Non-Cognizant Mode) モードで記録再生処理を実行する構成とすることが必要となる。

【0157】このためには、このデータ解析記録方式 (Cognizant Mode) と、データ非解析記録方式 (Non-Cognizant Mode) とをまったく別の記録方式とすることも一案ではあるが、この場合、1つの機器において両方のモードを選択的に実行可能とするためには、1機器に両モ

ードの実行処理構成を装備することが必要となり、これは、機器のコスト高を招くという問題がある。

【0158】そこで本発明の構成では、この2つの記録方式、すなわちデータ解析記録方式 (Cognizant Mode) と、データ非解析記録方式 (Non-Cognizant Mode) のいずれの方式を適用するかに応じて、コンテンツ暗号処理用の鍵を異なる鍵として生成して使用する構成とすることで、機器および記録方式に応じて2つの記録方式を明確に区別して、両方式が無秩序に混在して実行される事態を解消し、機器および記録方式に応じたいずれか一方の統一的な記録方式によるコンテンツ処理構成を、機器の装備および処理負荷を増大させることなく実現したものである。

【0159】具体的には、データ解析記録方式 (Cognizant Mode) 記録用の秘密情報 (再生時にも必要) としての暗号化、復号処理鍵生成用のキー (データ解析記録方式用キー (Cognizant Key)) をデータ解析記録方式 (Cognizant Mode) による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とし、一方、データ非解析記録方式 (Non-Cognizant Mode) 記録用の秘密情報 (再生時にも必要) としての暗号化、復号処理鍵生成用のキー (データ非解析記録方式用キー (Non-Cognizant Key)) を、データ非解析記録方式 (Non-Cognizant Mode) による記録または再生を行える機能を持つ機器にのみ提供して機器内に格納する構成とした。

【0160】本構成により、例えば、データ解析記録方式 (Cognizant Mode) で記録されたコンテンツについて、バグを原因として、あるいはデータの改竄、記録再生プログラムの不正改造等によって、データ非解析記録方式 (Non-Cognizant Mode) の記録再生機能のみを有する機器において、誤ってまたは不正な記録再生の実行を防止することができる。

【0161】図16、図17に戻って、コンテンツ記録処理の説明を続ける。記録再生装置1600は、さらに、使用するマスターキーの世代番号、すなわち、自身が格納するマスターキーの世代番号 [記録時世代番号 (Generation#n)] 1650を取得して、これを記録媒体1620に記録時世代番号1651として格納する。

【0162】ディスク上には、どのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー1605、記録モードフラグ1635、マスターキーの世代番号 [記録時世代番号 (Generation#n)] 1651を格納することができる。

【0163】なお、記録媒体1620には、予め、プレ (pre-recording) 世代番号が格納されており、プレ世代番号と同一またはプレ世代番号より新しい世代のマスターキーを用いて暗号化されて格納されたコンテンツのみの再生を可能とする構成となっている。この構成については、後段の再生処理の欄で説明する。

【0164】次にディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key)、あるいは、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key)、いずれかの組合せから、タイトル固有キー (Title Unique Key) を生成する。

【0165】すなわち、記録モードがデータ解析記録方式 (Cognizant Mode) である場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成し、記録モードがデータ非解析記録方式 (Non-Cognizant Mode) である場合には、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成する。

【0166】前述したように、データ解析記録方式 (Cognizant Mode) 記録用の秘密情報としての暗号化、復号処理鍵生成用のキー (データ解析記録方式用キー (Cognizant Key)) は、データ解析記録方式 (Cognizant Mode) による記録または再生を行える機能を持つ機器のみが有し、一方、データ非解析記録方式 (Non-Cognizant Mode) 記録用の秘密情報としての暗号化、復号処理鍵生成用のキー (データ非解析記録方式用キー (Non-Cognizant Key)) は、データ非解析記録方式 (Non-Cognizant Mode) による記録または再生を行える機能を持つ機器のみが有する。従って、一方の記録方式にのみ対応した機器においては、いずれか一方のモードのみを選択してコンテンツ記録が実行される。すなわち、データ解析記録方式用キー (Cognizant Key) を用いるか、あるいはデータ非解析記録方式用キー (Non-Cognizant Key) を用いるかの一方のみに限られることとなる。

【0167】しかし、両者のキーを格納し、両モードの記録方式を実行可能な機器においては、いずれのモードによる記録を実行するかを決定する処理が必要となる。このモード決定プロセス処理について、すなわち、コンテンツの記録をデータ解析記録方式 (Cognizant Mode) によって実行するか、データ非解析記録方式 (Non-Cognizant Mode) で実行するかを決定するプロセスについて図21を用いて説明する。

【0168】基本的には、コンテンツ記録は、できる限りデータ解析記録方式 (Cognizant Mode) によって実行するのが望ましい。これは、前述したように、EMI と埋め込みCCI (Embedded CCI) との不整合を生じさせないためである。ただし、前述したように、新規なデータフォーマットの出現等によるデータ解析エラー等の発生の可能性もあり、このような場合に、データ非解析記録方式 (Non-Cognizant Mode) での記録処理を実行する。

【0169】図21の各ステップについて説明する。ス

テップS5001では、記録装置は、データ・フォーマットを解析可能か否かを判定する。先に説明したように、埋め込みCCI (Embedded CCI) は、コンテンツの内部に埋め込まれており、データフォーマットの解析が不可能であれば、埋め込みCCI (Embedded CCI) の読み取りが不可能となるので、この場合は、データ非解析記録方式 (Non-Cognizant Mode) での記録処理を実行する。

【0170】データフォーマットの解析が可能であれば、ステップS5002に進み、記録装置が、データ (コンテンツ) のデコード処理、埋め込みCCI (Embedded CCI) の読み取り、更新処理が可能か否かを判定する。コンテンツおよび埋め込みCCI (Embedded CCI) は通常、符号化 (エンコード) されており、埋め込みCCI (Embedded CCI) の読み取りには復号 (デコード) を実行することが必要となる。例えば多チャンネル同時記録などの際に、復号回路が他に使用されているなど理由で、機器が復号処理可能でない場合は、埋め込みCCI (Embedded CCI) の読み取りができないので、データ非解析記録方式 (Non-Cognizant Mode) での記録処理を実行する。

【0171】ステップS5002のデータ (コンテンツ) のデコード処理、埋め込みCCI (Embedded CCI) の読み取り、更新処理が可能であると判定されると、ステップS5003において、記録装置に対するユーザ入力中に、データ非解析モードでの記録処理の実行指定入力があるか、否かが判定される。この処理は、ユーザの指定によるモード選択を可能とした機器においてのみ実行されるステップであり、通常の機器、すなわちユーザによるモード指定を許容しない機器においては実行されない。ユーザ入力によるデータ非解析記録方式 (Non-Cognizant Mode) での記録処理指定があった場合は、データ非解析記録方式 (Non-Cognizant Mode) での記録処理が実行される。

【0172】次に、ステップS5004において、コンテンツ packets (ex. 受信データ) 中に、データ非解析モードでの記録処理の実行指定があるか否かが判定される。データ中にデータ非解析モードでの記録処理の実行指定がある場合は、データ非解析記録方式 (Non-Cognizant Mode) での記録処理が実行される。指定がない場合は、データ解析記録方式 (Cognizant Mode) での記録処理が実行される。

【0173】データ解析記録方式 (Cognizant Mode) での記録処理、およびデータ非解析記録方式 (Non-Cognizant Mode) での記録処理の双方を選択的に実行可能な機器においては、上述したモード決定プロセス処理によって、いずれのモードでの記録を実行するかが決定される。ただし、図21の処理フローからも理解されるように、データ解析記録方式 (Cognizant Mode) での記録が可能な場合は、基本的にデータ解析記録方式 (Cognizant

t Mode)での処理が実行されることになる。

【0174】前述したように、記録モードをデータ解析記録方式 (Cognizant Mode)とした場合は、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) からタイトル固有キー (Title Unique Key) を生成し、記録モードをデータ非解析記録方式 (Non-Cognizant Mode)とした場合は、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とからタイトル固有キー (Title Unique Key) を生成する。

【0175】タイトル固有キー (Title Unique Key) 生成の具体的な方法を図22に示す。図22に示すように、ブロック暗号関数を用いたハッシュ関数にタイトルキー (Title Key) とディスク固有キー (Disc Unique Key) と、データ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode)の場合)、もしくは、データ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode)の場合)を入力して得られた結果を用いる例1の方法、あるいは、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とデータ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode)の場合)もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode)の場合)とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをタイトル固有キー (Title Unique Key) として使用する例2の方法が適用できる。

【0176】なお、上記の説明では、マスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデータ解析記録方式用キー (Cognizant Key)もしくはデータ非解析記録方式用キー (Non-Cognizant Key)からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とディスクID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key)もしくはデータ非解析記録方式用キー (Non-Cognizant Key)から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスターキー (Master Key) とディスクID (Disc ID) と、データ解析記録方式用キー (Cognizant Key)もしくはデータ非解析記録方式用キー (Non-Cognizant Key)からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0177】たとえば上記の5CDTCPに規定される

伝送フォーマットのひとつを使用した場合、データはMPEG2のTSパケットで伝送される場合がある。たとえば、衛星放送を受信したセットトップボックス (STB: Set Top Box) がこの放送を記録機に5CDTCPを用いて伝送する際に、STBは衛星放送通信路で伝送されたMPEG2 TSパケットをIEEE1394上も伝送することが、データ変換の必要がなく望ましい。

【0178】記録再生装置1600は記録すべきコンテンツデータをこのTSパケットの形で受信し、前述したTS処理手段300において、各TSパケットを受信した時刻情報であるATSを付加する。なお、先に説明したように、ブロックデータに付加されるブロック・シードは、ATSとコピー制御情報、さらに他の情報を組み合わせた値から構成してもよい。

【0179】ATSを付加したTSパケットをX個 (例えばX=32) 並べて、1ブロックのブロックデータが形成 (図5の上の図参照) され、図16、17の下段に示すように、被暗号化データとして入力されるブロックデータの先頭の第1~4バイトが分離され (セクタ1608) て出力される32ビットのATSを含むブロックシード (Block Seed) と、先に生成したタイトル固有キー (Title Unique Key) とから、そのブロックのデータを暗号化する鍵であるブロック・キー (Block Key) が生成1607される。

【0180】ブロック・キー (Block Key) の生成方法の例を図23に示す。図23では、いずれも32ビットのブロック・シード (Block Seed) と、64ビットのタイトル固有キー (Title Unique Key) とから、64ビットのブロックキー (Block Key) を生成する例を2つ示している。

【0181】上段に示す例1は、鍵長64ビット、入出力がそれぞれ64ビットの暗号関数を使用している。タイトル固有キー (Title Unique Key) をこの暗号関数の鍵とし、ブロックシード (Block Seed) と32ビットの定数 (コンスタント) を連結した値を入力して暗号化した結果をブロックキー (Block Key) としている。

【0182】例2は、FIPS 180-1のハッシュ関数SHA-1を用いた例である。タイトル固有キー (Title Unique Key) とブロックシード (Block Seed) を連結した値をSHA-1に入力し、その160ビットの出力を、たとえば下位64ビットのみ使用するなど、64ビットに縮約したものをブロックキー (Block Key) としている。

【0183】なお、上記ではディスク固有キー (Disc Unique Key)、タイトル固有キー (Title Unique Key)、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにマスターキー (Master Key) とスタンパーID (Stamper ID) とディ

スクID (Disc ID) とタイトルキー (Title Key) とブロックシード (Block Seed) と、データ解析記録方式用キー (Cognizant Key) (Cognizant Mode の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) を用いてブロックキー (Block Key) を生成してもよい。

【0184】ブロックキーが生成されると、生成されたブロックキー (Block Key) を用いてブロックデータを暗号化する。図16、17の下段に示すように、ブロックシード (Block Seed) を含むブロックデータの先頭の第1～mバイト (たとえばm=8) は分離 (セクタ1608) されて暗号化対象とせず、m+1バイト目から最終データまでを暗号化1609する。なお、暗号化されないmバイト中にはブロック・シードとしての第1～4バイトも含まれる。セクタ1608により分離された第m+1バイト以降のブロックデータは、暗号処理手段150に予め設定された暗号化アルゴリズムに従って暗号化1609される。暗号化アルゴリズムとしては、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) を用いることができる。

【0185】また、前述したようにブロック・シードには、コピー制限情報 (CCI : Copy Control Information) を含ませることが可能であり、データ解析記録方式 (Cognizant Mode) での記録処理を実行した場合には、コンテンツデータ内部に埋め込まれたコピー制御情報 (CCI) である埋め込みCCI (Embedded CCI) に対応するコピー制御情報が記録され、また、データ非解析記録方式 (Non-Cognizant Mode) での記録処理を実行した場合には、図20で説明したパケットヘッダ上のEMI (Encryption Mode Indicator) を反映したコピー制御情報が記録される。

【0186】すなわち、データ解析記録方式 (Cognizant Mode) による情報記録処理の場合、データ部内の埋め込みコピー制御情報 (CCI) に基づくコピー制御情報を含むブロックシードを、1以上のパケットからなるブロックデータに付加した記録情報生成処理を実行し、データ非解析記録方式 (Non-Cognizant Mode) による情報記録処理の場合、パケットに含まれるコピー制御情報としてのエンクリプション・モード・インディケータ (EMI) に基づくコピー制御情報を含むブロックシードを、1以上のパケットからなるブロックデータに付加した記録情報生成処理を実行する。

【0187】ここで、使用する暗号アルゴリズムのブロック長 (入出力データサイズ) がDESのように8バイトであるときは、Xを例えば32とし、mを例えば8の倍数とすることで、端数なくm+1バイト目以降のブロックデータ全体が暗号化できる。

【0188】すなわち、1ブロックに格納するTSパケットの個数をX個とし、暗号アルゴリズムの入出力デー

タサイズをLバイトとし、nを任意の自然数とした場合、 $192 \times X = m + n \times L$ が成り立つようにX、m、Lを定めることにより、端数処理が不要となる。

【0189】暗号化した第m+1バイト以降のブロックデータは暗号処理のされていない第1～mバイトデータとともにセクタ1610により結合されて暗号化コンテンツ1612として記録媒体1620に格納される。

【0190】以上の処理により、コンテンツはブロック単位で、世代管理されたマスターキー、ATSを含むブロック・シード等に基づいて生成されるブロック鍵で暗号化が施されて記録媒体に格納される。

【0191】上述のように、本構成では、世代管理されたマスターキーによりコンテンツデータが暗号化され記録媒体に格納されているので、その記録媒体を他の記録再生器における再生処理は、少なくとも同一世代、あるいはデータを記録した際に使用されたマスターキーの世代より新しい世代を有する記録再生器であることが復号、すなわち再生可能となる条件となる。

【0192】さらに、ブロックキーは上述のようにデータ解析記録方式 (Cognizant Mode) の記録の場合は、データ解析記録方式用キー (Cognizant Key) に基づいて生成され、データ非解析記録方式 (Non-Cognizant Mode) の記録の場合は、データ非解析記録方式用キー (Non-Cognizant Key) に基づいて生成される。これらの暗号化データは、記録時と同一のモードに対応する鍵 (データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key)) を持つ機器でのみ再生可能となる。

【0193】すなわち、データ解析記録方式用キー (Cognizant Key) は、記録時にストリーム中に埋め込まれた Embedded CCI を認識して必要に応じて更新する能力を持つ機器およびそのデータの再生を許された機器にのみ与えられ、この鍵を持たない機器ではデータ解析記録方式 (Cognizant Mode) で記録されたコンテンツの再生は行えない。

【0194】同様に、データ非解析記録方式用キー (Non-Cognizant Key) は、記録時にストリーム中の埋め込みCCI (Embedded CCI) を認識しないデータ非解析記録方式 (Non-Cognizant) の記録モードの機能を持つ機器と、そのモードで記録されたデータの再生を許された機器にのみ与えられ、この鍵を持たない機器ではデータ非解析記録方式 (Non-Cognizant Mode) で記録されたコンテンツの再生は行えないようになっている。なお、再生処理の詳細については後述する。

【0195】次に図18に示すフローチャートに従って、データ記録処理にともなって実行されるTS処理手段300におけるATS付加処理および暗号処理手段150における暗号処理の処理全体の流れをまとめて説明する。図18のS1801において、記録再生装置は自身のメモリ180に格納しているマスターキーおよびデ

ータ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode) の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) を読み出す。また、ディスクからスタンパー ID (Stamper ID) を読み出す。

【0196】S1802において、記録媒体に識別情報としてのディスク ID (Disc ID) が既に記録されているかどうかを検査する。記録されていればS1803でこのディスク ID を読出し、記録されていない場合はS1804で、ランダムに、もしくはあらかじめ定められた方法でディスク ID を生成し、ディスクに記録する。次に、S1805では、マスターキーとスタンパー ID (Stamper ID) とディスク ID を用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数 SHA-1 を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

【0197】次にS1806に進み、その一回の記録ごとの固有の鍵としてのタイトルキー (Title Key) を生成し、記録モード (Recording Mode) とマスターキーの世代番号とともにディスクに記録する。記録モード (Recording Mode) は、実行する情報記録モードが、データ解析記録方式 (Cognizant Mode) であるか、データ非解析記録方式 (Non-Cognizant Mode) であるかを示す。

【0198】次にS1807で、上記のディスク固有キーとタイトルキーと、データ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode) の場合) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) から、タイトル固有キーを生成する。

【0199】タイトル固有キーの生成の詳細フローを図24に示す。暗号処理手段150は、ステップS2001において、記録モードにより分岐する。この分岐は、記録再生器のプログラムや、記録再生器を使用するユーザによって入力された指示データに基づいて判定される。

【0200】S2001で記録モードがデータ解析記録方式 (Cognizant Mode)、すなわち、Cognizant 記録の場合は、ステップS2002に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) とから、タイトル固有キー (Title Unique Key) を生成する。

【0201】S2001で記録モードがデータ非解析記録方式 (Non-Cognizant Mode)、すなわち、Non-Cognizant 記録の場合は、ステップS2003に進みディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、SHA-1 を用いる方法やブ

ロック暗号に基づくハッシュ関数を使用する。

【0202】S1808では、記録再生装置は記録すべきコンテンツデータの被暗号化データをTSパケットの形で受信する。S1809で、TS処理手段300は、各TSパケットを受信した時刻情報であるATSを付加する。あるいはコピー制御情報CCIとATS、さらに他の情報を組み合わせた値を付加する。次に、S1810で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS1811に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0203】次に、暗号処理手段150は、S1812で、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS1807で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【0204】S1813では、ブロックキーを用いてS1811で形成したブロックデータを暗号化する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) が適用される。

【0205】S1814で、暗号化したブロックデータを記録媒体に記録する。S1815で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS1808に戻って残りのデータの処理を実行する。

【0206】上述の処理にしたがって、コンテンツの記録処理がデータ解析記録方式 (Cognizant Mode) あるいは、データ非解析記録方式 (Non-Cognizant Mode) のいずれかによって実行される。コンテンツの記録処理がデータ解析記録方式 (Cognizant Mode) で実行される場合は、コンテンツの暗号化に適用される鍵が、データ解析記録方式用キー (Cognizant Key) に基づいて生成され、また、コンテンツの記録処理がデータ非解析記録方式 (Non-Cognizant Mode) で実行される場合は、コンテンツの暗号化に適用される鍵がデータ非解析記録方式用キー (Non-Cognizant Key) に基づいて生成されることになる。従って、それぞれの方式においてディスクに記録されたコンテンツは、記録時に使用したデータ解析記録方式用キー (Cognizant Key)、あるいはデータ非解析記録方式用キー (Non-Cognizant Key) のいずれか、同一のキーを適用して復号用の鍵を生成することが必須となり、各方式が混在した記録、再生処理が防止される。

【0207】次に、上記のようにして記録媒体に記録された暗号化コンテンツを復号して再生する処理について

図25の処理ブロック図と、図26～図28のフローチャートを用いて説明する。

【0208】図25の処理ブロック図を参照しながら、図26に示すフローチャートに従って、復号処理および再生処理について、処理の流れを説明する。図26のS2401において、記録再生装置2300（図25参照）はディスク2320からディスクID2302とブレ（pre-recording）記録世代番号とスタンパーID（Stamper ID）2380を読み出し、また自身のメモリからマスターキー2301、データ解析記録方式用キー（Cognizant Key）2331および／あるいはデータ非解析記録方式用キー（Non-Cognizant Key）2332を読み出す。先の記録処理の説明から明らかなように、ディスクIDはディスクにあらかじめ記録されているか、そうでない場合は記録再生器において生成してディスクに記録したディスク固有の識別子である。

【0209】ブレ（pre-recording）記録世代番号2360は、予め記録媒体であるディスクに格納されたディスク固有の世代情報である。このブレ（pre-recording）世代番号と、データ記録時のマスターキーの世代番号、すなわち記録時世代番号2350を比較して再生処理の可否を制御する。マスターキー2301は、図14のフローにより記録再生装置のメモリに格納され世代管理のなされた秘密キーである。データ解析記録方式用キー（Cognizant Key）およびデータ非解析記録方式用キー（Non-Cognizant Key）は、それぞれデータ解析（Cognizant）記録モードおよびデータ非解析（Non-Cognizant）記録モードに対応したシステム共通の秘密キーである。

【0210】記録再生装置2300は、次に、S2402で、ディスクから読み出すべきデータのタイトルキー、さらに、データの記録モード、データを記録したときに使用したマスターキーの世代番号（Generation #）すなわち記録時世代番号2350を読み出す。次に、S2403で読み出すべきデータが再生可能か否かを判定する。判定の詳細フローを図27に示す。

【0211】図27のステップS2501において、記録再生装置は、S2401で読み出したブレ世代番号と、S2402で読み出した記録時世代番号の新旧を判定する。記録時世代番号が示す世代が、ブレ記録世代情報が表す世代以後でないと判定された場合、即ち、データ記録時世代情報が表す世代が、ブレ記録世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップS2404乃至S2409をスキップして、再生処理を行わずに処理を終了する。従って、記録媒体に記録されたコンテンツが、ブレ記録世代情報が表す世代よりも古い世代のマスターキーに基づいて暗号化されたものである場合には、その再生は許可されず、再生は行われない。

【0212】即ち、この処理は、不正が発覚して、最新の世代のマスターキーが与えられなくなった不正な記録

装置で、古い世代のマスターキーに基づいて、データが暗号化され、記録媒体に記録された場合に該当するものと判断し、そのような不正な装置によってデータが記録された記録媒体の再生は行わないとした処理である。これにより、不正な記録装置の使用を排除することができる。

【0213】一方、ステップS2501において、記録時世代番号が表す世代が、ブレ記録世代番号が表す世代以後であると判定された場合、即ち、記録時世代情報が表す世代が、ブレ記録世代番号が表す世代nと同一か、または新しい世代であり、従って、記録媒体に記録されたコンテンツが、ブレ記録世代情報が表す世代以後の世代のマスターキーに基づいて暗号化されたものである場合には、ステップS2502に進み、記録再生装置は、自身のメモリが記憶している暗号化マスターキーCの世代情報を取得し、その暗号化マスターキーの世代と、暗号時世代情報が表す世代を比較して、その世代の前後を判定する。

【0214】ステップS2502において、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代以後でないと判定された場合、即ち、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代よりも古い世代である場合、再生不可能と判断し、ステップS2404乃至S2409をスキップして、再生処理を行わずに処理を終了する。

【0215】一方、ステップS2502において、メモリに記憶された暗号化マスターキーCの世代が、記録時世代情報が表す世代以後であると判定された場合、即ち、メモリに記憶されたマスターキーCの世代が、記録時世代情報が表す世代と同一か、またはそれよりも新しい場合、ステップS2503に進み、記録時のモードに対応する鍵、すなわちデータ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）を、再生機器自身が所有しているかどうかを判断する。

【0216】ステップS2503において、記録時のモードに対応する鍵であるデータ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）を、再生機器自身が所有している場合、再生可能と判定する。記録時のモードに対応する鍵（データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key））を、再生機器自身が所有していない場合、再生不可能と判定する。

【0217】再生可能と判定された場合は、ステップS2404に進む。S2404では、ディスクID（Disc ID）とマスターキー（Master Key）とスタンパーID（Stamper ID）を用いてディスク固有キー（Disc Unique Key）を生成2302する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1

に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key) として使用する方や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID) を入力して得られた結果を用いるなどの方法が挙げられる。ここで使用するマスターキーは、図26のステップS2402で記録媒体から読み出した、そのデータの記録時世代番号が表す世代(時点)のマスターキーである。もし記録再生装置がこれよりも新しい世代のマスターキーを保持している場合には、前述した方法を用いて記録時世代番号が表す世代のマスターキーを作成し、それを用いてディスク固有キー (Disc Unique Key) を生成してもよい。

【0218】次に、S2405で、タイトル固有キーの生成を行なう。タイトル固有キーの生成の詳細フローを図28に示す。暗号処理手段150は、ステップS2601において、記録モードの判定を実行する。この判定は、ディスクから読み出した記録モード (Recording Mode) に基づいて実行される。

【0219】S2601において、記録モードがデータ解析記録方式 (Cognizant Mode) であると判定された場合は、ステップS2602に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) とから、タイトル固有キー (Title Unique Key) を生成する。

【0220】S2601において、記録モードがデータ非解析記録方式 (Non-Cognizant Mode) であると判定された場合は、ステップS2603に進み、ディスク固有キー (Disc Unique Key) とタイトルキー (Title Key) と、データ非解析記録方式用キー (Non-Cognizant Key) とから、タイトル固有キー (Title Unique Key) を生成する。キー生成には、SHA-1を用いる方やブロック暗号に基づくハッシュ関数を使用する。

【0221】なお、上記の説明では、マスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてマスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、マスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Dis

cID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0222】次にS2406でディスクから暗号化されて格納されている暗号化コンテンツ2312から順次ブロックデータ (Block Data) を読み出し、S2407で、ブロックデータの先頭の4バイトのブロック・シード (Block Seed) をセレクト2310において分離して、ブロックシード (Block Seed) と、S2405で生成したタイトル固有キーを用いてブロックキーを生成する。

【0223】ブロック・キー (Block Key) の生成方法は、先に説明した図23の構成を適用することができる。すなわち、32ビットのブロック・シード (Block Seed) と、64ビットのタイトル固有キー (Title Unique Key) とから、64ビットのブロックキー (Block Key) を生成する構成が適用できる。

【0224】なお、上記説明ではディスク固有キー (Disc Unique key) 、タイトル固有キー (Title Unique Key) 、ブロックキー (Block Key) をそれぞれ生成する例を説明したが、たとえば、ディスク固有キー (Disc Unique Key) とタイトル固有キー (Title Unique Key) の生成を実行することなく、ブロックごとにマスターキー (Master Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) とタイトルキー (Title Key) と、ブロックシード (Block Seed) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) を用いてブロックキー (Block Key) を生成してもよい。

【0225】ブロックキーが生成されると、次にS2408で、ブロックキー (Block Key) を用いて暗号化されているブロックデータを復号2309し、セレクト2308を介して復号データとして出力する。なお、復号データには、トランスポートストリームを構成する各トランスポートパケットにATSが付加されており、先に説明したTS処理手段300において、ATSに基づくストリーム処理が実行される。その後、データは、使用、たとえば、画像を表示したり、音楽を再生したりすることが可能となる。

【0226】このように、ブロック単位で暗号化され記録媒体に格納された暗号化コンテンツはブロック単位でATSを含むブロック・シードに基づいて生成されるブロック鍵で復号処理が施されて再生が可能となる。ブロックキーを用いて暗号化されているブロックデータを復号し、S2409で、全データを読み出したかを判断し、全データを読み出していれば終了し、そうでなければS2406に戻り残りのデータを読み出す。

【0227】なお、上述した記録再生装置は、図25に示すように、データ解析記録方式 (Cognizant Mode) 記

録用の暗号化、復号処理鍵生成用のキー（データ解析記録方式用キー（Cognizant Key））と、データ非解析記録方式（Non-Cognizant Mode）記録用の暗号化、復号処理鍵生成用のキー（データ非解析記録方式用キー（Non-Cognizant Key））との双方を選択的に使用可能な構成例であるが、先に図29、図30に示して説明したように、いずれか一方のキー、すなわちデータ解析記録方式用キー（Cognizant Key）、あるいはデータ非解析記録方式用キー（Non-Cognizant Key）のみを格納した機器においては、いずれか一方のみの格納キーに対応する方式のみを実行し、格納キーに基づいてコンテンツの復号処理用のブロックキーを生成する。

【0228】[5. メディアキーを用いた暗号処理によるコンテンツの記録再生]ところで、上記の実施例においては、有効化キーブロック（EKB: EnablingKey Block）を用いて各記録再生装置に対してマスターキーを伝送し、これを用いて記録再生装置がデータの記録、再生を行うとしていた。

【0229】マスターキーは、その時点におけるデータの記録全体に有効な鍵であり、ある時点のマスターキーを得ることができた記録再生装置は、その時点およびそれ以前にこのシステムで記録されたデータを復号することが可能になる。ただし、システム全体で有効であるというその性質上、マスターキーが攻撃者に露呈した場合の影響がシステム全体に及ぶという不具合もある。

【0230】これに対し、記録媒体のEKB（Enabling Key Block）を用いて伝送する鍵を、全システムに有効なマスターキーではなく、その記録媒体にのみ有効なメディアキーとすることにより、キーの露呈の影響を抑えることが可能となる。以下に、第2の実施例としてマスターキーの代わりにメディアキーを用いる方式を説明する。ただし、第1の実施例との変更部分のみを説明する。

【0231】図29には、図13と同様の例として、デバイス0が記録媒体に格納されているt時点のEKBと自分があらかじめ格納しているリーフキーK0000とノードキーK000、K00を用いて更新ノードキーK(t)00を生成し、これを用いて更新メディアキー: K(t) mediaを得る様子を示している。ここで得たK(t) mediaは、その記録媒体のデータの記録、再生時に使用される。

【0232】なお、図29におけるプレ記録世代番号(Generation #n)は、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので必須ではなくオプションとして設定される。

【0233】各記録再生装置は、たとえば、データの記録もしくは再生のために記録媒体が記録再生装置に挿入された際に、図30に示すフローチャートによってその記録媒体用のメディアキー: K(t) mediaを計算し、後にその記録媒体へのアクセスに使用する。

【0234】図30のステップS2801のEKBの読みこみとS2802のEKBの処理は、それぞれ図14のステップS1403およびS1404と同様の処理である。

【0235】ステップS2803において記録再生装置はメディアキーK(t) mediaをノードキーK(t)00で暗号化した暗号文Enc(K(t)00, K(t) media)を記録媒体から読みこみ、ステップS2804でこれを復号してメディアキーを得る。もしこの記録再生装置が図11に示すツリー構成のグループから排除、すなわちリボークされていれば、メディアキーを入手できず、その記録媒体への記録および再生が行えない。

【0236】次に、メディアキーを適用してキーを生成して、生成したキーによる暗号処理を行なって記録媒体へデータを記録する処理について説明するが、メディアキーにおいてはマスターキーのように世代の新旧という概念はないので、第1の実施例において図15に示した、プレ記録世代情報と記録再生装置自身が格納するマスターキーの世代の比較による記録可能かどうかのチェックは行わず、上記処理においてメディアキーを得られていれば記録を行えると判断する。すなわち、図31に示す処理フローのようになる。図31の処理フローは、メディアキーの取得をS2901で判定し、取得された場合にのみ、ステップS2902においてコンテンツの記録処理を実行するものである。

【0237】メディアキーを用いた暗号処理によるコンテンツデータの記録処理の様子を、図32、33のブロック図および図34のフローチャートを用いて説明する。

【0238】本実施例では、第1の実施例と同様、記録媒体として光ディスクを例とする。この実施例では、記録媒体上のデータのbit-by-bitコピーを防ぐために、記録媒体固有の識別情報としてのディスクID(Disc ID)を、データを暗号化する鍵に作用させるようにしている点も同様である。

【0239】図32および図33は、それぞれ第1の実施例における図16および図17に対応する図であり、マスターキー(Master Key)の代わりにメディアキー(Media Key)が使われている点が異なっており、また、マスターキーの世代を示す記録時世代番号(Generation #)を用いていない点が異なっている。図32および図33の差異は、図16、図17の差異と同様ディスクIDの書き込みを実行するかしないかの差異である。

【0240】図34はメディアキーを用いる本実施例におけるデータ記録処理を示すものであり、前述した図18(実施例1)のフローチャートに対応する。以下、図34の処理フローについて実施例1と異なる点を中心として説明する。

【0241】図34のS3201において、記録再生装置3000は自身のメモリに格納しているデータ解析

記録方式用キー (Cognizant Key) および／もしくはデータ非解析記録方式用キー (Non-Cognizant Key) と、図 30 の S 2 8 0 4 で計算し、一時的に保存しているメディアキー K (t) media を読み出す。また、ディスクからスタンパー I D (Stamper ID) を読み出す。

【0242】 S 3 2 0 2 において、記録再生装置は記録媒体 (光ディスク) 3 0 2 0 に識別情報としてのディスク I D (Disc ID) が既に記録されているかどうかを検査する。記録されていれば、S 3 2 0 3 でこのディスク I D (Disc ID) を読出し (図 3 2 に相当)、記録されていないければ、S 3 2 0 4 で、ランダムに、もしくはあらかじめ定められた方法でディスク I D (Disc ID) を生成し、ディスクに記録する (図 3 3 に相当)。ディスク I D (Disc ID) はそのディスクにひとつあればよいので、リードインエリアなどに格納することも可能である。いずれの場合でも、次に S 3 2 0 5 に進む。

【0243】 S 3 2 0 5 では、S 3 2 0 1 で読み出したメディアキーとスタンパー I D (Stamper ID) とディスク I D (Disc ID) を用いて、ディスク固有キー (Disc Unique Key) を生成する。ディスク固有キー (Disc Unique Key) の具体的な生成方法としては、第 1 の実施例で使用方法と同じ方法で、マスターキーの代わりにメディアキーを使用すればよい。

【0244】 次に S 3 2 0 6 に進み、その一回の記録ごとに固有の鍵：タイトルキー (Title Key) をランダムに、あるいはあらかじめ定められた方法で生成し、ディスクに記録する。同時に、このタイトル (データ) を記録したときの記録モード (Recording Mode) をディスクに記録する。

【0245】 ディスク上には、どこかのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー、Recording Mode を格納することができる。

【0246】 ステップ S 3 2 0 7 乃至 S 3 2 1 5 は図 18 の S 1 8 0 7 乃至 S 1 8 1 5 と同様であるため説明を省略する。

【0247】 なお、上記の説明では、メディアキー (Media Key) とスタンパー I D (Stamper ID) とディスク I D (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) とデータ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキー (Media Key) とスタンパー I D (Stamper ID) とディスク I D (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー

(Title Key) を用いずに、メディアキー (Media Key) とスタンパー I D (Stamper ID) とディスク I D (Disc ID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0248】 以上のようにして、メディアキーを用いて記録媒体にデータを記録することができる。

【0249】 次に、上記のようにして記録されたデータを再生する処理の様子を図 3 5 のブロック図と図 3 6 のフローチャートを用いて説明する。

【0250】 図 3 5 は、第 1 の実施例における図 2 5 に対応する図であり、マスターキー (Master Key) の変わりにメディアキー (Media Key) が使われ、そのため記録時世代番号 (Generation #) が省略されている点が異なっている。

【0251】 図 3 6 の S 3 4 0 1 において、記録再生装置 3 4 0 0 は記録媒体であるディスク 3 4 2 0 からスタンパー I D (Stamper ID) およびディスク I D (Disc ID) を、また自身のメモリからデータ解析記録方式用キー (Cognizant Key) および／あるいはデータ非解析記録方式用キー (Non-Cognizant Key) と、図 3 0 の S 2 8 0 4 で計算し一時的に保存しているメディアキーを読み出す。

【0252】 なお、この記録媒体の挿入時に、図 3 0 の処理を行い、メディアキーを入手できなかった場合には、再生処理を行わずに終了する。

【0253】 次に S 3 4 0 2 で、ディスクから読み出すべきデータのタイトルキー (Title Key) とこのデータを記録した際の記録モード Recording Mode を読み出す。

【0254】 次に S 3 4 0 3 で、このデータが再生可能であるか否かを判断する。S 3 4 0 3 の処理の詳細を図 3 7 に示す。

【0255】 ステップ S 3 5 0 1 ではメディアキー (Media Key) を得られたか否かを判定する。メディアキーを得られなかった場合、再生不可能となり、メディアキーを得られた場合はステップ S 3 5 0 2 に進む。ステップ S 3 5 0 2 の処理は図 2 7 の S 2 5 0 3 と同じであり、そのデータの記録時に使われた記録モードに対応する鍵 (データ解析記録方式 (Cognizant Mode) の場合、データ解析記録方式用キー (Cognizant Key)、データ非解析記録方式 (Non-Cognizant Mode) の場合、データ非解析記録方式用キー (Non-Cognizant Key)) を再生機器が持っている場合には「再生可能」と判断してステップ S 3 4 0 4 に進み、それ以外の場合には、「再生不可能」と判断して、ステップ S 3 4 0 4 乃至 S 3 4 0 9 をスキップして、再生処理を行わずに処理を終了する。

【0256】 ステップ S 3 4 0 4 乃至 S 3 4 0 9 の処理は、図 2 6 の S 2 4 0 4 乃至 S 2 4 0 9 と同様であるため、説明を省略する。

【0257】なお、上記の説明では、メディアキー (Media Key) と スタンパーID (Stamper ID) とディスクID (Disc ID) からディスク固有キー (Disc Unique Key) を生成し、これとタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) をそれぞれ生成するようにしているが、ディスク固有キー (Disc Unique Key) を不要としてメディアキー (Media Key) とスタンパーID (Stamper ID) とディスクID (Disc ID) とタイトルキー (Title Key) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) から直接タイトル固有キー (Title Unique Key) を生成してもよく、また、タイトルキー (Title Key) を用いずに、メディアキー (Media Key) と スタンパーID (Stamper ID) とディスクID (Disc ID) と、データ解析記録方式用キー (Cognizant Key) もしくはデータ非解析記録方式用キー (Non-Cognizant Key) からタイトル固有キー (Title Unique Key) 相当の鍵を生成してもよい。

【0258】上記のようにして、記録媒体へのデータの記録および記録媒体からの再生処理が実行される。

【0259】[6. LSIキーを用いた暗号処理によるコンテンツの記録再生] 次に、LSIキーを用いた暗号処理によるコンテンツの記録再生装置および処理構成について説明する。LSIキーは、記録再生装置内で実行する暗号化処理または復号処理を実行する暗号処理手段 (図1, 図2参照) としての暗号化/復号LSIに対応して設定され、LSI内に格納されるキーであり、例えば同一仕様のLSIに共通のキーとして格納される。あるいは所定のLSI製造単位 (ロット単位) にのみ共通のキーとしてもよい。

【0260】LSIキーを用いた記録再生処理を実行する記録再生装置としてHDR (Hard Disk Recorder) を例にあげて説明する。まず、LSIキーを用いた暗号処理によるコンテンツデータの記録処理の様子を、図38のブロック図および図39のフローチャートを用いて説明する。

【0261】HDR (Hard Disk Recorder) は、データ記録再生メディア (記録媒体) としてハードディスク (HD) を有する。この実施例では、図38に示すように、ハードディスクレコーダ (HDR) にハードディスクドライブ (HDD) が装着され、ハードディスクドライブ (HDD) 内のハードディスク (HD) に対してデータ記録、再生を行なう構成を持つ装置を例として説明する。HDR (Hard Disk Recorder) 3500は、暗号化/復号LSIを有し、暗号化/復号LSI内にLSIキー3501を内蔵している。また、ハードディスクドライブ (HDD) 3520には、ハードディスクドライブ (HDD) 352

0に対して設定されたキーであるドライブキー3521が格納される。また、ハードディスク (HD) 3540には、メディアキー3541が格納される。このメディアキーは、前述のEKB配信されるキーではなく、ハードディスク (HD) 3540の製造時にハードディスク (HD) 3540固有のキーとして各HDに格納されるキーである。

【0262】図39はLSIキーを用いる本実施例におけるデータ記録処理を示すものであり、前述した図18のフローチャートに対応する。以下、図39の処理フローについて説明する。

【0263】図39のS3501において、記録再生装置3500は自身のメモリに格納しているデータ解析記録方式用キー (Cognizant Key) および/もしくはデータ非解析記録方式用キー (Non-Cognizant Key) を読み出し、暗号処理手段としてのLSIからLSIキー3501を読み出す。また、ハードディスクドライブ (HDD) 3520に対して設定されたキーであるドライブキー3521、ハードディスク (HD) 3540固有のキーとして設定されたメディアキー3541を読み出す。

【0264】S3502において、その一回の記録ごとに固有の鍵: タイトルキー (Title Key) をランダムに、あるいはあらかじめ定められた方法で生成し、ディスクに記録する。同時に、このタイトル (データ) を記録したときの記録モード (Recording Mode) をディスクに記録する。

【0265】ディスク上には、どこのデータがどんなタイトルを構成するかという情報が格納されたデータ管理ファイルがあり、このファイルにタイトルキー、Recording Mode を格納することができる。

【0266】S3503におけるタイトル固有キー (Title Unique Key) の生成処理について、図40を用いて説明する。図40に示すように、ブロック暗号関数を用いたハッシュ関数にLSIキー、タイトルキー (Title Key)、ドライブキー、メディアキー、およびデータ解析記録方式用キー (Cognizant Key) (データ解析記録方式 (Cognizant Mode) の場合)、もしくは、データ非解析記録方式用キー (Non-Cognizant Key) (データ非解析記録方式 (Non-Cognizant Mode) の場合) を順次入力し、各出力との排他論理和を実行して、繰り返し暗号処理を実行して得られた結果をタイトル固有キー (Title Unique Key) とする構成が可能である。

【0267】ステップS3504乃至S3511は図18のS1808乃至S1815と同様であるため説明を省略する。

【0268】以上のようにして、LSIキーを用いて記録媒体にデータを記録することができる。

【0269】次に、上記のようにして記録されたデータを再生する処理を図41のブロック図と図42のフローチャートを用いて説明する。

【0270】図42のS3701において、記録再生装置3500は自身のメモリに格納しているデータ解析記録方式用キー (Cognizant Key) および／もしくはデータ非解析記録方式用キー (Non-Cognizant Key) を読み出し、暗号処理手段としてのLSIからLSIキー3501を読み出す。また、ハードディスクドライブ (HDD) 3520に対して設定されたキーであるドライブキー3521、ハードディスク (HD) 3540固有のキーとして設定されたメディアキー3541を読み出す。

【0271】次にS3702で、ディスクから読み出すべきデータのタイトルキー (TitleKey) とこのデータを記録した際の記録モード Recording Mode を読み出す。

【0272】ステップS3703におけるタイトル固有キー (Title Unique Key) の生成処理は、図40を用いて説明したと同様の処理である。ステップS3704乃至S3707の処理は、図26のS2406乃至S2409と同様であるため、説明を省略する。

【0273】上記のようにして、記録媒体へのデータの記録および記録媒体からの再生処理が実行される。

【0274】[7. コピー制御]

(記録処理におけるコピー制御) さて、コンテンツの著作権者等の利益を保護するには、ライセンスを受けた装置において、コンテンツのコピーを制御する必要がある。

【0275】即ち、コンテンツを記録媒体に記録する場合には、そのコンテンツが、コピーしても良いもの (コピー可能) かどうかを調査し、コピーして良いコンテンツだけを記録するようにする必要がある。また、記録媒体に記録されたコンテンツを再生して出力する場合には、その出力するコンテンツが、後で、違法コピーされないようにする必要がある。

【0276】そこで、そのようなコンテンツのコピー制御を行いながら、コンテンツの記録再生を行う場合の図1または図2の記録再生装置の処理について、図43および図44のフローチャートを参照して説明する。

【0277】まず、外部からのデジタル信号のコンテンツを、記録媒体に記録する場合においては、図43

(A) のフローチャートにしたがった記録処理が行われる。図43 (A) の処理について説明する。図1の記録再生器100を例として説明する。デジタル信号のコンテンツ (デジタルコンテンツ) が、例えば、IEEE1394シリアルバス等を介して、入出力I/F120に供給されると、ステップS4001において、入出力I/F120は、そのデジタルコンテンツを受信し、ステップS4002に進む。

【0278】ステップS4002では、入出力I/F120は、受信したデジタルコンテンツが、コピー可能であるかどうかを判定する。即ち、例えば、入出力I/F120が受信したコンテンツが暗号化されていない場合 (例えば、上述のDTCPを使用せずに、平文のコン

テンツが、入出力I/F120に供給された場合) には、そのコンテンツは、コピー可能であると判定される。

【0279】また、記録再生装置100がDTCPに準拠している装置であるとし、DTCPに従って処理を実行するものとする。DTCPでは、コピーを制御するためのコピー制御情報としての2ビットのEMI (Encryption Mode Indicator) が規定されている。EMIが00B (Bは、その前の値が2進数であることを表す) である場合は、コンテンツがコピーフリーのもの (Copy-free) であることを表し、EMIが01Bである場合には、コンテンツが、それ以上のコピーをすることができないもの (No-more-copies) であることを表す。さらに、EMIが10Bである場合は、コンテンツが、1度だけコピーして良いもの (Copy-one-generation) であることを表し、EMIが11Bである場合には、コンテンツが、コピーが禁止されているもの (Copy-never) であることを表す。

【0280】記録再生装置100の入出力I/F120に供給される信号にEMIが含まれ、そのEMIが、Copy-freelyやCopy-one-generationであるときには、コンテンツはコピー可能であると判定される。また、EMIが、No-more-copiesやCopy-neverであるときには、コンテンツはコピー可能でないと判定される。

【0281】ステップS4002において、コンテンツがコピー可能でないと判定された場合、ステップS4003～S4005をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0282】また、ステップS4002において、コンテンツがコピー可能であると判定された場合、ステップS4003に進み、以下、ステップS4003～S4005において、図3 (A) のステップS302、S303、S304における処理と同様の処理が行われる。すなわち、TS処理手段300によるトランスポートパケットに対するATS付加、暗号処理手段150における暗号化処理が実行され、その結果得られる暗号化コンテンツを、記録媒体195に記録して、記録処理を終了する。

【0283】なお、EMIは、入出力I/F120に供給されるデジタル信号に含まれるものであり、デジタルコンテンツが記録される場合には、そのデジタルコンテンツとともに、EMI、あるいは、EMIと同様にコピー制御状態を表す情報 (例えば、DTCPにおけるembedded CCIなど) も記録される。

【0284】この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。

【0285】本発明の記録再生装置では、このEMIやembedded CCIなどのコピー制御情報を、TSパケットに

付加する形で記録する。即ち、図10の例2や例3のように、ATSを24ビットないし30ビット分と、コピー制御情報を加えた32ビットを図5に示すように各TSパケットに付加する。

【0286】外部からのアナログ信号のコンテンツを、記録媒体に記録する場合においては、図43(B)のフローチャートにしたがった記録処理が行われる。図43(B)の処理について説明する。アナログ信号のコンテンツ(アナログコンテンツ)が、入出力I/F140に供給されると、入出力I/F140は、ステップS4011において、そのアナログコンテンツを受信し、ステップS4012に進み、受信したアナログコンテンツが、コピー可能であるかどうかを判定する。

【0287】ここで、ステップS4012の判定処理は、例えば、入出力I/F140で受信した信号に、マクロビジョン(Macrovision)信号や、CGMS-A(Copy Generation Management System-Analog)信号が含まれるかどうかに基づいて行われる。即ち、マクロビジョン信号は、VHS方式のビデオカセットテープに記録すると、ノイズとなるような信号であり、これが、入出力I/F140で受信した信号に含まれる場合には、アナログコンテンツは、コピー可能でないと判定される。

【0288】また、例えば、CGMS-A信号は、デジタル信号のコピー制御に用いられるCGMS信号を、アナログ信号のコピー制御に適用した信号で、コンテンツがコピーフリーのもの(Copy-freely)、1度だけコピーして良いもの(Copy-one-generation)、またはコピーが禁止されているもの(Copy-never)のうちのいずれであるかを表す。

【0289】従って、CGMS-A信号が、入出力I/F140で受信した信号に含まれ、かつ、そのCGMS-A信号が、Copy-freelyやCopy-one-generationを表している場合には、アナログコンテンツは、コピー可能であると判定される。また、CGMS-A信号が、Copy-neverを表している場合には、アナログコンテンツは、コピー可能でないと判定される。

【0290】さらに、例えば、マクロビジョン信号も、CGMS-A信号も、入出力I/F4で受信した信号に含まれない場合には、アナログコンテンツは、コピー可能であると判定される。

【0291】ステップS4012において、アナログコンテンツがコピー可能でないと判定された場合、ステップS4013乃至S4017をスキップして、記録処理を終了する。従って、この場合には、コンテンツは、記録媒体10に記録されない。

【0292】また、ステップS4012において、アナログコンテンツがコピー可能であると判定された場合、ステップS4013に進み、以下、ステップS4013乃至S4017において、図3(B)のステップS322乃至S326における処理と同様の処理が行われ、こ

れにより、コンテンツがデジタル変換、MPEG符号化、TS処理、暗号化処理がなされて記録媒体に記録され、記録処理を終了する。

【0293】なお、入出力I/F140で受信したアナログ信号に、CGMS-A信号が含まれている場合に、アナログコンテンツを記録媒体に記録するときには、そのCGMS-A信号も、記録媒体に記録される。即ち、図10で示したCCIもしくはその他の情報の部分に、この信号が記録される。この際、一般的には、Copy-One-Generationを表す情報は、それ以上のコピーを許さないよう、No-more-copiesに変換されて記録される。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0294】(再生処理におけるコピー制御)次に、記録媒体に記録されたコンテンツを再生して、デジタルコンテンツとして外部に出力する場合においては、図44(A)のフローチャートにしたがった再生処理が行われる。図44(A)の処理について説明する。まず最初に、ステップS4101、S4102、S4103において、図4(A)のステップS401、S402、S403における処理と同様の処理が行われ、これにより、記録媒体から読み出された暗号化コンテンツが暗号処理手段150において復号処理がなされ、TS処理がなされる。各処理が実行されたデジタルコンテンツは、バス110を介して、入出力I/F120に供給される。

【0295】入出力I/F120は、ステップS4104において、そこに供給されるデジタルコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI、あるいは、EMIと同様にコピー制御状態を表す情報(コピー制御情報)が含まれない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0296】また、例えば、入出力I/F120に供給されるデジタルコンテンツにEMI等のコピー制御情報が含まれる場合、従って、コンテンツの記録時に、DTCIPの規格にしたがって、EMI等のコピー制御情報が記録された場合には、そのEMI(記録されたEMI(Recorded EMI))等のコピー制御情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。また、EMI等のコピー制御情報が、No-more-copiesであるときには、コンテンツは、後でコピー可能なものでないと判定される。

【0297】なお、一般的には、記録されたEMI等のコピー制御情報が、Copy-one-generationやCopy-neverであることはない。Copy-one-generationのEMIは記録時にNo-more-copiesに変換され、また、Copy-neverのEMIを持つデジタルコンテンツは、記録媒体に記録

されないからである。ただし、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」などのルールが決められている場合は、この限りではない。

【0298】ステップS4104において、コンテンツが、後でコピー可能なものであると判定された場合、ステップS4105に進み、入出力I/F120は、そのデジタルコンテンツを、外部に出力し、再生処理を終了する。

【0299】また、ステップS4104において、コンテンツが、後でコピー可能なものでないと判定された場合、ステップS4106に進み、入出力I/F120は、例えば、DTC Pの規格等にしがって、デジタルコンテンツを、そのデジタルコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0300】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合には、コンテンツは、それ以上のコピーは許されない。

【0301】このため、入出力I/F120は、DTC Pの規格にしたがい、相手の装置との間で認証を相互に行い、相手が正当な装置である場合（ここでは、DTC Pの規格に準拠した装置である場合）には、デジタルコンテンツを暗号化して、外部に出力する。

【0302】次に、記録媒体に記録されたコンテンツを再生して、アナログコンテンツとして外部に出力する場合においては、図44（B）のフローチャートにしたがった再生処理が行われる。図44（B）の処理について説明する。ステップS4111乃至S4115において、図4（B）のステップS421乃至S425における処理と同様の処理が行われる。すなわち、暗号化コンテンツの読み出し、復号処理、TS処理、MPEGデコード、D/A変換が実行される。これにより得られるアナログコンテンツは、入出力I/F140で受信される。

【0303】入出力I/F140は、ステップS4116において、そこに供給されるコンテンツが、後でコピー可能なものかどうかを判定する。即ち、例えば、記録されていたコンテンツにEMI等のコピー制御情報がいっしょに記録されていない場合には、そのコンテンツは、後でコピー可能なものであると判定される。

【0304】また、コンテンツの記録時に、たとえばDTC Pの規格にしたがって、EMI等のコピー制御情報

が記録された場合には、その情報が、Copy-freelyであるときには、コンテンツは、後でコピー可能なものであると判定される。

【0305】また、EMI等のコピー制御情報が、No-more-copiesである場合、もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合には、コンテンツは、後でコピー可能なものでないと判定される。

【0306】さらに、例えば、入出力I/F140に供給されるアナログコンテンツにCGMS-A信号が含まれる場合、従って、コンテンツの記録時に、そのコンテンツとともにCGMS-A信号が記録された場合には、そのCGMS-A信号が、Copy-freelyであるときには、アナログコンテンツは、後でコピー可能なものであると判定される。また、CGMS-A信号が、Copy-neverであるときには、アナログコンテンツは、後でコピー可能なものでないと判定される。

【0307】ステップS4116において、コンテンツが、後でコピー可能であると判定された場合、ステップS4117に進み、入出力I/F140は、そこに供給されたアナログ信号を、そのまま外部に出力し、再生処理を終了する。

【0308】また、ステップS4116において、コンテンツが、後でコピー可能でないと判定された場合、ステップS4118に進み、入出力I/F140は、アナログコンテンツを、そのアナログコンテンツが後でコピーされないような形で外部に出力し、再生処理を終了する。

【0309】即ち、例えば、上述のように、記録されたEMI等のコピー制御情報が、No-more-copiesである場合（もしくは、システムにおいてたとえば「Copy-one-generationのコピー制御情報は、No-more-copiesに変換せずに記録するが、No-more-copiesとして扱う」というルールが決められていて、その条件下で記録されたEMI等のコピー制御情報がCopy-one-generationである場合）には、コンテンツは、それ以上のコピーは許されない。

【0310】このため、入出力I/F140は、アナログコンテンツを、それに、例えば、マクロビジョン信号や、Copy-neverを表すCGMS-A信号を付加して、外部に出力する。また、例えば、記録されたCGMS-A信号が、Copy-neverである場合にも、コンテンツは、それ以上のコピーは許されない。このため、入出力I/F140は、CGMS-A信号をCopy-neverに変更して、アナログコンテンツとともに、外部に出力する。

【0311】以上のように、コンテンツのコピー制御を行いながら、コンテンツの記録再生を行うことにより、

コンテンツに許された範囲外のコピー（違法コピー）が行われることを防止することが可能となる。

【0312】[8. 再暗号化を不要としたコンテンツコピーまたは格納処理] 上述したコピー制御の手法を用いたデータ記録処理は、外部から入力されるデータが基本的に暗号化されていないデータである場合の処理を中心として説明している。外部から入力されるデータが暗号化データ（コンテンツ）であった場合は、入力暗号データを復号し、その後、前述したマスターキー、メディアキー、LSIキー等に基づいてタイトル固有キーを生成し、タイトル固有キーに基づくブロックキーを適用してデータの再暗号化処理を行なった後、記録することになる。

【0313】しかし、機器間におけるデータコピー処理、あるいはインターネット、衛星等のデータ配信手段を介して記録再生装置にデータを格納する場合にあっては、データ（コンテンツ）転送は暗号化されて実行されるのがより安全であり、また、記録再生装置において復号処理や、再暗号化処理を実行するのは、データコピー、または格納処理の効率を低下させることになる。

【0314】データ出力元および出力先となる2つの記録再生装置がライセンスを受け、双方がコンテンツを正当に利用することが認められた機器である場合、このような機器間でのデータコピーまたはデータ移動は、データ供給元の記録再生装置の記録媒体に格納されている暗号化コンテンツを復号、再暗号化せずに直接、データ提供先の記録再生装置に格納した方が効率的である。また、インターネット、衛星等のデータ配信手段を介して記録再生装置にデータを格納する場合においても、データを受信して格納する場合、記録再生装置がライセンスを受けコンテンツの利用可能な機器であれば、コンテンツの再暗号化処理を実行せずに格納処理のみを実行する方が効率的なデータ受信、格納処理ができる。以下、このような機器間のデータコピーまたはデータ移動処理、あるいはインターネット、衛星等のデータ配信手段を介して記録再生装置にデータを格納する場合において、コンテンツの再暗号化を実行せずに記録媒体に格納し、かつ、自己の記録再生装置において利用可能な復号キーを得ることを可能とした構成について説明する。

【0315】(8. 1. 機器間のコンテンツコピー) まず、記録再生装置から他の記録再生装置に対するコンテンツコピー処理について説明する。一例として、LSIキーを適用してタイトル固有キーを生成する処理を行なって、ハードディスクに暗号化コンテンツを格納するHDR (Hard Disk recorder) をデータ送信機器とし、マスターキーを適用してタイトル固有キーを生成する処理を行なって、記録媒体に暗号化コンテンツを格納するDVR (Digital Versatile RAM) システムをデータ受信機器として実行されるコンテンツコピーまたはコンテンツ移動処理について説明する。

【0316】図45にデータ送信機器であるHDRシステムのコンテンツ出力時の処理、図47にデータ受信機器であるDVRシステムのコンテンツ入力時の処理を示し、図46にHDRシステムのコンテンツ出力時の処理フロー、図48にDVRシステムのコンテンツ入力時の処理フローを示す。まず、図46の処理フローに従って、HDRシステムのコンテンツ出力時の処理について説明する。

【0317】ステップS5101において、コンテンツの送信機器と受信機器間において相互認証処理および鍵交換処理が実行される。これは、互いに相手の正当性を確認するため処理である。実行される相互認証のプロトコル例としては、ISO/IEC 9798-2に代表される、共通鍵暗号を用いるもの、ISO/IEC 9798-3に代表される、公開鍵暗号を用いるもの、ISO/IEC 9798-4に代表される、暗号学的チェック関数 (MAC) を用いるものなどが挙げられる。

【0318】図49は、暗号学的チェック関数 (MAC) を用いた相互認証および暗号鍵共有のための方法のひとつを本実施例に用いたものである。

【0319】図49において、コンテンツの送信機器と受信機器に対応するデバイスA、Bは、共通の鍵 K_{ab} を格納している。まず、デバイスBは乱数 R_b を発生し、デバイスAに送る。なお、図49における記号「|」は連結を表している。

【0320】次にデバイスAは、乱数 R_a 、 S_a を生成し、 R_a 、 S_a とともに $MAC(K_{ab}, R_a || R_b || S_a)$ をデバイスBに送る。 $MAC(K_{ab}, R_a || R_b || S_a)$ は、暗号学的チェック関数に鍵として K_{ab} を、データとして $R_a || R_b || S_a$ を入力することを表す。暗号学的チェック関数は、ISO/IEC 9797に示されているように、FIPS 46-2のデータ暗号化規格 (Data Encryption Standard, DES) を用いて構成することが可能である。

【0321】デバイスBは、受信したデータを用いて自分でも $MAC(K_{ab}, R_a || R_b || S_a)$ を計算し、これが受信したものと一致するかを検査する。一致すれば通信相手であるデバイスAが正当であると認め、処理を続けるが、一致しなければ不正なものと判断して処理を中止する。

【0322】次にデバイスBは乱数 S_b を生成し、これと $MAC(K_{ab}, R_b || R_a || S_b)$ をデバイスAに送る。デバイスAも受信したデータを用いて自分で $MAC(K_{ab}, R_b || R_a || S_b)$ を計算し、受信したものと一致するかを確認する。一致すれば通信相手であるデバイスBが正当であると認め、処理を続けるが、一致しなければ不正なものと判断して処理を中止する。最後に、双方が $MAC(K_{ab}, S_a || S_b)$ を計算し、これをそのセッションにおけるセッションキーとして使用する。

【0323】上記のようにすることにより、コンテンツ

送信機器と受信機器としての2つの記録再生装置は互いの正当性を検査することができ、またセッションキーを安全に共有することができる。

【0324】図50は、公開鍵暗号を用いた認証技術を実施例に適用したものである。図50において、デバイスA、Bは、それぞれ自分の公開鍵(PubKey)、秘密鍵(PriKey)を持っている。さらに、各デバイスは、リボケーションリスト(Rev)、レジストレーションリスト(Reg)を有している。リボケーションリストは、不正者リストあるいはブラックリストとも呼ばれ、例えばその装置の秘密鍵が露呈してしまったもののIDがリストアップされ、単調増加するバージョンナンバーとともにセンタ(キー発行機関)のデジタル署名が施されたリストである。レジストレーションリストは、正当者リストあるいは登録リストとも呼ばれ、その時点で信頼できる(秘密が露呈していない)装置のIDがリストアップされ、単調増加するバージョンナンバーとともにセンタ(キー発行機関)のデジタル署名が施されたリストである。

【0325】図50において、デバイスBは乱数Rbを発生させ、デバイスAに送る。デバイスAは、乱数Kaを発生させ、楕円曲線E上でシステム共通の点(ベースポイント)であるGとKaを乗算してVaを計算し、さらに自分の秘密鍵(PriKeyA)を用いてデータRa||Rb||Va||RevVa||RegVaに対して施した署名とともに、公開鍵証明書他のデータ(CertA||Ra||Rb||Va)をデバイスBに送る。

【0326】デバイスBは、デバイスAの公開鍵証明書(CertA)の正当性、および署名の正当性を検査する。そして、自分がリボケーションリストを格納していれば、相手のIDがリボケーションリストに載っていないことを、また、自分がレジストレーションリストを格納していれば、相手のIDがレジストレーションリストに登録されていることを確認する。以上の確認が正常にできなければ、デバイスBはデバイスAが不正者と判断して処理を終了する。以上の確認が正常にできれば、デバイスBは、乱数Kbを生成して、キー発行機関が行ったのと同様な計算を行い、公開鍵証明書他のデータ(CertB||Rb||Ra||Vb)とともに自分の秘密鍵(PriKeyB)を用いてデータRb||Ra||Vb||RevVb||RegVbに対して施した署名データをデバイスAに送る。

【0327】この後、デバイスAではKaとVbを、デバイスBではKbとVaを、それぞれ楕円曲線E上で乗算してセッションキーKsを得る。

【0328】上述のような手法により、コンテンツの送信側機器と受信側機器間で相互認証がなされ、セッションキーKsが保持される。図46に戻り、処理フローの説明を続ける。ステップS5101における相互認証が成立したか否かがステップS5102において判定され、

認証不成立の場合は、以後の処理は実行されず、処理は中止される。認証が成立した場合は、ステップS5103において、記録再生装置(HDR)3500(図45参照)は自身のメモリに格納しているデータ解析記録方式用キー(Cognizant Key)および/もしくはデータ非解析記録方式用キー(Non-Cognizant Key)を読み出し、暗号処理手段としてのLSIからLSIキー3501を読み出す。また、ハードディスクドライブ(HDD)3520に対して設定されたキーであるドライブキー3521、ハードディスク(HD)3540固有のキーとして設定されたメディアキー3541を読み出す。

【0329】次にS5104で、ディスクから読み出すべきデータのタイトルキー(TitleKey)とこのデータを記録した際の記録モードRecording Modeを読み出す。

【0330】ステップS5105におけるタイトル固有キー(Title Unique Key)の生成処理は、図40を用いて説明したと同様の処理である。

【0331】次に、ステップS5106において、タイトル固有キー、記録モードを前述のステップS5101で取得したセッション鍵で暗号化して、コンテンツ受信機器に対して送信する。さらに、ステップS5107において、暗号化コンテンツを記録媒体(本例の場合はハードディスク3540)から読み出してコンテンツ受信機器に対して送信する。なお、この暗号化コンテンツは、コンテンツの送信側機器である記録再生装置(HDR)3500のLSIキー他に基づいて生成されたタイトル固有キーによって暗号化されたコンテンツである。ステップS5108において、全ブロックデータの読み出し完了を確認して処理を終了する。

【0332】一方、暗号化コンテンツを受信し、格納する記録再生装置における処理について、図47、図48を参照して説明する。ここでは、コンテンツ受信機器がDVRシステムであると想定して説明する。図48の処理フローの各ステップについて説明する。ステップS5201、S5202は、送信側と受信側機器間で実行される相互認証、鍵交換処理であり、図46の説明と同様の処理である。

【0333】相互認証が成立すると、コンテンツ受信機器であるDVRシステムは、ステップS5203において、記録再生装置自身のメモリに格納しているマスターキーおよびデータ解析記録方式用キー(Cognizant Key)(データ解析記録方式(Cognizant Mode)の場合)もしくはデータ非解析記録方式用キー(Non-Cognizant Key)(データ非解析記録方式(Non-Cognizant Mode)の場合)を読み出す。また、ディスクからスタンパーID(Stamper ID)を読み出す。

【0334】S5204において、記録媒体に識別情報としてのディスクID(Disc ID)が既に記録されているかどうかを検査する。記録されていればS5205でこのディスクIDを読み出し、記録されていなければS5

206で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S5207では、マスタキーとスタンパーID(Stamper ID)とディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

【0335】次にS5208に進み、コンテンツ送信側機器から暗号化されたタイトル固有キーと、記録モードを受信して、先の認証処理において取得したセッション鍵を用いて復号する。

【0336】次に、ステップS5209において、タイトルキーの生成処理を実行し、記録モードと共にディスク1620(図47参照)に格納する。タイトルキーの生成処理について、図51を参照して説明する。

【0337】図51に示すように、タイトルキーの生成は、先に図22例1で説明したタイトル固有キーの生成処理の逆方向の処理として実行される。すなわち、前述したブロックキーの生成処理に対応する暗号処理シーケンスの一部を構成するタイトル固有キーの生成処理シーケンスを逆方向処理とした処理(復号処理)として実行される。具体的には、コンテンツ送信機器から受信したタイトル固有キーを、ディスク固有キーを用いて64bitブロック暗号関数の逆関数により復号し、これをデータ解析記録方式用キー(Cognizant Key)(データ解析記録方式(Cognizant Mode)の場合)もしくはデータ非解析記録方式用キー(Non-Cognizant Key)(データ非解析記録方式(Non-Cognizant Mode)の場合)と排他論理和し、さらに、ディスク固有キーを用いて64bitブロック暗号関数の逆関数を適用して復号した結果としてタイトルキーを生成する。

【0338】ステップS5209では、上述の処理において、生成したタイトルキーを記録モードと共にディスクに格納する。次にステップS5210において、コンテンツ送信機器から受信した暗号化コンテンツをそのままディスクに格納する。なお、この暗号化コンテンツは、コンテンツ送信機器において生成したタイトル固有キーに基づいて生成されるブロックキーで暗号化したコンテンツであり、復号処理や再暗号化処理はなされていないデータである。ステップS5210では、全データの受信を確認し、処理を終了する。

【0339】上述の処理において、データ受信側機器であるDVRシステムは、データ送信側機器であるHDRシステムにおいて生成したタイトル固有キーに基づいて生成されるブロックキーで暗号化したコンテンツを格納することになる。

【0340】しかし、暗号化コンテンツを受信して格納したDVRシステムは、コンテンツ送信機器であるHDRシステムからタイトル固有キーを受信して、受信した

タイトル固有キーに基づいて、タイトルキーを生成し、タイトルキーをディスクに格納する処理を実行している。先に説明した図22のタイトル固有キー生成処理を実行することで、HDRシステムにおいて生成したと同じタイトル固有キーを生成することが可能となり、ディスクに格納した暗号化コンテンツの復号が可能となる。

【0341】なお、上述の説明では、64bitブロック暗号関数を暗号処理、復号処理用関数として適用した例を説明し、例えば前述の図22での説明において、タイトル固有キーの大きさは、図22の例1で使用するブロック暗号関数の出力サイズと同じ64bitという前提とした。しかし、これを図23の例1に示すブロックキー生成用の暗号関数の鍵として用いる場合、たとえば暗号関数としてFIPS 46-2に規定されるDES(Data Encryption Standard)を用いたい場合、DESの鍵長は56ビットであるため、図22で生成した64ビットのタイトル固有キーを56ビットに縮約することが必要となる。

【0342】縮約処理の一例について図52を用いて説明する。図52(A)に示すように、64ビットのタイトル固有キーを8つの8ビットブロック $a_1, a_2, a_3, \dots, a_8$ に分割し、 a_i と a_{i+1} の排他論理和(XOR)を縮約されたタイトル固有キーの第 i 番目の8ビットブロック b_i にする。この方法により、図22で生成した64ビットのタイトル固有キーを56ビットに縮約することが可能となる。

【0343】タイトル固有キーがこのようにして縮約されている場合、受信側のデバイス(例えばDVRシステム)ではまず、タイトル固有キーの縮約をもどす、伸張の処理を行う必要がある。なぜなら、先に説明した図51に示すタイトルキーの導出に用いる暗号関数の逆関数の入力64ビットだからである。この伸張処理は図52(B)に示す方法によって行うことができる。

【0344】すなわち、まず伸張後の64ビットのうちの第1の8ビットの c_1 を任意の値として決め、これと伸張前の第1の8ビットである b_1 を排他論理和(XOR)した値を c_2 とする。また c_2 と b_2 を排他論理和(XOR)した値を c_3 とする。以下同様に、 $c_i \text{ XOR } b_i$ の値を c_{i+1} とするものである。このようにすることにより、 c_1, c_2, \dots, c_8 は a_1, a_2, \dots, a_8 と同一値になることの保証はないものの、 $(c_1 \text{ XOR } (c_2))$ は $(a_1 \text{ XOR } (a_2))$ の値と同じ b_1 になる。すなわち $(a_i \text{ XOR } (a_{i+1})) = (c_i \text{ XOR } (c_{i+1})) = b_i$ という関係が成り立つものとなる。よって、 a_1, a_2, \dots, a_8 と c_1, c_2, \dots, c_8 のいずれも、図52(A)の縮約方式を用いて縮約を行ったときに、同一の値を出力するように構成することが可能である。

【0345】なお、縮約の方式には、図52(A)に示

したもののみならず、たとえば64ビットのタイトル固有キーの上位56ビットを使用するなどの方法も考えられるが、この場合には、伸張方式として、与えられた56ビットの下位に任意の8ビットの値を連結したものを出力する方式を考えればよい。

【0346】次に、コンテンツ送信機器をDVRシステムとして、コンテンツ受信機器をHDRシステムとした例について説明する。すなわち、マスターキーを適用してタイトル固有キーを生成して暗号化コンテンツを格納する処理を実行するDVR (Digital Versatile RAM) システムから、LSIキーを適用してタイトル固有キーを生成してハードディスクに暗号化コンテンツを格納するHDR (Hard Disk recorder) に対するコンテンツコピーまたはコンテンツ移動処理について説明する。

【0347】図53にデータ送信機器であるDVRシステムのコンテンツ出力時の処理、図55にデータ受信機器であるHDRシステムのコンテンツ入力時の処理を示し、図54にDVRシステムのコンテンツ出力時の処理フロー、図56にHDRシステムのコンテンツ入力時の処理フローを示す。まず、図54の処理フローに従って、DVRシステムのコンテンツ出力時の処理について説明する。

【0348】ステップS5301において、コンテンツの送信機器と受信機器間において相互認証処理および鍵交換処理が実行される。これは、互いに相手の正当性を確認するため処理である。実行される相互認証のプロトコル例としては、先に説明したように、ISO/IEC 9798-2に代表される、共通鍵暗号を用いるもの、ISO/IEC 9798-3に代表される、公開鍵暗号を用いるもの、ISO/IEC 9798-4に代表される、暗号学的チェック関数 (MAC) を用いるものなどが挙げられる。

【0349】上述の各手法により、コンテンツの送信側機器と受信側機器間で相互認証がなされ、セッション鍵Ksが保持される。ステップS5301における相互認証が成立したか否かがステップS5302において判定され、認証不成立の場合は、以後の処理は実行されず、処理は中止される。認証が成立した場合は、ステップS5303において、記録再生装置 (DVR) 1600 (図53参照) はディスクからディスクIDとプレ (pre-recording) 記録世代番号とスタンパーID (Stamper ID)を読み出し、また自身のメモリからマスターキー、データ解析記録方式用キー (Cognizant Key)あるいはデータ非解析記録方式用キー (Non-Cognizant Key)を読み出す。

【0350】次に、S5304で、ディスクから読み出すべきデータのタイトルキー、さらに、データの記録モード、データを記録したときに使用したマスターキーの世代番号 (Generation #) すなわち記録時世代番号を読み出す。次に、S5305で読み出すべきデータが再生可能か否かを判定する。判定の詳細は、先に説明した図

27のフローおよびその説明を参照されたい。

【0351】再生不可能と判断された場合は、ステップS5305以下をスキップして、再生処理を行わずに処理を終了する。再生可能と判定された場合は、ステップS5306に進む。S5306では、ディスクID (Disc ID) とマスターキー (Master Key) とスタンパーID (Stamper ID)を用いてディスク固有キー (Disc Unique Key)を生成する。このキー生成方法は、例えば、FIPS 180-1で定められているハッシュ関数SHA-1に、マスターキーとディスクID (Disc ID) とのビット連結により生成されるデータを入力し、その160ビットの出力から必要なデータ長のみをディスク固有キー (Disc Unique Key)として使用方法や、ブロック暗号関数を用いたハッシュ関数にマスターキー (Master Key) とディスクID (Disc ID)を入力して得られた結果を用いるなどの方法が挙げられる。

【0352】次に、S5307で、タイトル固有キーの生成を行なう。タイトル固有キーの生成は、例えば先に説明した図22の処理構成による。次に、ステップS5308において、タイトル固有キー、記録モードを前述のステップS5301で取得したセッション鍵で暗号化して、コンテンツ受信機器に対して送信する。さらに、ステップS5309において、暗号化コンテンツを記録媒体 (本例の場合はDVD-RAMディスク1620) から読み出してコンテンツ受信機器に対して送信する。なお、この暗号化コンテンツは、コンテンツの送信側機器である記録再生装置 (DVR) 1600のマスターキー他に基つて生成されたタイトル固有キーによって暗号化されたコンテンツである。ステップS5310において、全ブロックデータの読み出し完了を確認して処理を終了する。

【0353】一方、暗号化コンテンツを受信し、格納する記録再生装置における処理について、図55、図56を参照して説明する。ここでは、コンテンツ受信機器がHDRシステムであると想定して説明する。図56の処理フローの各ステップについて説明する。ステップS5401、S5402は、送信側と受信側機器間で実行される相互認証、鍵交換処理であり、図54の説明と同様の処理である。

【0354】相互認証が成立すると、コンテンツ受信機器であるHDRシステムは、ステップS5403において、記録再生装置3500 (図55参照) は自身のメモリに格納しているデータ解析記録方式用キー (Cognizant Key)および/もしくはデータ非解析記録方式用キー (Non-Cognizant Key)を読み出し、暗号処理手段としてのLSIからLSIキー3501を読み出す。また、ハードディスクドライブ (HDD) 3520に対して設定されたキーであるドライブキー3521、ハードディスク (HD) 3540固有のキーとして設定されたメディアキー3541を読み出す。

【0355】S5404において、コンテンツ送信側機器から暗号化されたタイトル固有キーと、記録モードを受信して、先の認証処理において取得したセッション鍵を用いて復号する。

【0356】次に、ステップS5405において、タイトルキーの生成処理、を実行し、記録モードと共にディスク3540（図55参照）に格納する。タイトルキーの生成処理について、図57を参照して説明する。

【0357】図57に示すように、タイトルキーの生成は、先に図40で説明したタイトル固有キーの生成処理の逆方向の処理として実行される。すなわち、前述したブロックキーの生成処理に対応する暗号処理シーケンスの一部を構成するタイトル固有キーの生成処理シーケンスを逆方向処理とした処理（復号処理）として実行される。具体的には、コンテンツ送信機器から受信したタイトル固有キーを、LSIキーを用いて64bitブロック暗号関数の逆関数により復号し、これをデータ解析記録方式用キー（Cognizant Key）（データ解析記録方式（Cognizant Mode）の場合）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）（データ非解析記録方式（Non-Cognizant Mode）の場合）と排他論理和し、さらに、出力に対してメディアキー、ドライブキーを順次、排他論理和、およびLSIキーを適用した64bitブロック暗号関数による復号を実行して結果としてタイトルキーを生成する。

【0358】ステップS5405では、上述の処理において、生成したタイトルキーを記録モードと共にディスクに格納する。次にステップS5406において、コンテンツ送信機器から受信した暗号化コンテンツをそのままディスクに格納する。なお、この暗号化コンテンツは、コンテンツ送信機器において生成したタイトル固有キーに基づいて生成されるブロックキーで暗号化したコンテンツであり、復号処理や再暗号化処理はなされていないデータである。ステップS5407では、全データの受信を確認し、処理を終了する。

【0359】上述の処理において、データ受信側機器であるHDRシステムは、データ送信側機器であるDVRシステムにおいて生成したタイトル固有キーに基づいて生成されるブロックキーで暗号化したコンテンツを格納することになる。

【0360】しかし、暗号化コンテンツを受信して格納したHDRシステムは、コンテンツ送信機器であるDVRシステムからタイトル固有キーを受信して、受信したタイトル固有キーに基づいて、タイトルキーを生成し、タイトルキーをディスクに格納する処理を実行している。先に説明した図40のタイトル固有キー生成処理を実行することで、DVRシステムにおいて生成したと同じタイトル固有キーを生成することが可能となり、ディスクに格納した暗号化コンテンツの復号が可能となる。

【0361】なお、上述の例では、HDRからDVR、DVRからHDRへのコンテンツコピー処理について説明したが、その他の機器間のコピー処理も同様の考え方によって実行できる。すなわち、データ送信側機器からデータ受信側機器に暗号化コンテンツに対応するタイトル固有キーを入力して、データ受信側機器において、タイトル固有キーに基づいてタイトルキーを生成して、コンテンツに対応付けて記録媒体に格納する。

【0362】すなわち、外部から入力する入力暗号データとしてのコンテンツに対して設定されるタイトル固有キーを第1暗号鍵とし、タイトル固有キーの復号処理により取得可能なタイトルキーを第2暗号鍵としたとき、入力される第1暗号鍵としてのタイトル固有キーに基づいて、記録再生装置に予め設定された記録媒体格納データの復号鍵生成処理シーケンスの少なくとも一部シーケンスを逆方向処理とした復号処理を実行して第2暗号鍵としてのタイトルキーを生成して、記憶媒体に格納する。暗号化コンテンツの復号時には、記録再生装置に予め設定された復号鍵生成処理シーケンスに従って、マスターキー、メディアキー、LSIキーのいずれかと、タイトルキー等を用いてタイトル固有キーを生成し、さらにブロックキーを生成して復号処理が実行される。

【0363】なお、前述したDVR等の情報処理装置では、図16他に示すように、ディスク固有キー（Disc Unique Key）の生成とタイトル固有キー（Title Unique Key）の生成処理を区別して行う構成例を説明したが、これをまとめて1つの関数として、マスターキー（Master Key）もしくはメディアキー（Media Key）と、スタンパID（Stamper ID）と、ディスクID（Disc ID）と、タイトルキー（Title Key）と、データ解析記録方式用キー（Cognizant Key）もしくはデータ非解析記録方式用キー（Non-Cognizant Key）から、図40に示す処理構成と同様の処理に従ってタイトル固有キー（Title Unique Key）を生成する構成としてもよい。このような構成とした場合においても、図51と同様の方式により、既知の値からタイトルキー（Title Key）を導出することが可能である。

【0364】なお、機器間でのコンテンツコピーを行うときに、前述したコピー制御情報CCIを更新すべきかしくなくてもよいかという問題が発生するが、例えば、特定の個人に属する機器間のコピーであるなどの条件の下にコピーが行われる場合などに限り、上述の復号、再暗号化処理を許容し、ブロックシードに格納されたCCIを更新しないコピーを実行可能とする構成としてもよい。また、CCIをブロックシード以外の付帯データとして格納し、その付帯データとしてのCCIの更新を実行する構成としてもよい。このような付帯データにCCIを持つ構成とすれば、機器間のコンテンツコピー時にコンテンツデータの復号、再暗号化を行わないでCCIの更新が可能となる。

【0365】(8. 2. 配信コンテンツの格納処理) 次に、インターネット、衛星等を介して配信される暗号化コンテンツを記録再生装置の記録媒体に格納する処理構成について説明する。

【0366】ここでは、コンテンツ提供サーバにおいて暗号化されたコンテンツをインターネット、衛星等を介してDVR (Digital Versatile RAM) システムのディスクに格納する例を説明する。なお、コンテンツ提供サーバは、先に図1、図2で説明したデータ記録再生装置構成と同様の構成にインターネット、衛星等を介したデータ配信可能な通信インタフェース、さらに、データ配信先の機器のIDを格納したデータベース、コンテンツを格納データベースを備えた構成によって実現される。なお、具体的ハードウェア構成については、後段で説明する。

【0367】図58にデータ送信側サイトのコンテンツ提供サーバにおけるコンテンツ出力時の処理、図60にデータ受信機器であるDVRシステムのコンテンツ入力時の処理を示し、図59にサーバのコンテンツ出力時の処理フロー、図61にDVRシステムのコンテンツ入力時の処理フローを示す。図59の処理フローに従って、サーバのコンテンツ出力時の処理について説明する。

【0368】コンテンツ提供サーバの処理は、図59に示すように、(a) コンテンツの暗号化処理、(b) 暗号化コンテンツデータ送信処理、(c) タイトル固有キー送信処理の3つの処理を行なう。まず、(a) コンテンツの暗号化処理について説明する。

【0369】ステップS6101において、コンテンツ提供サーバ3800 (図58参照) は、タイトル固有キーを生成し、記録モードを決定する。タイトル固有キーは、例えば乱数、疑似乱数を発生させて生成する。記録モードは、データ解析記録方式 (Cognizant Mode)、もしくはデータ非解析記録方式 (Non-Cognizant Mode) のいずれかに決定するが、コンテンツデータに含まれるコピー制御情報 (CCI : Copy Control Information) について、サーバがコンテンツデータの暗号化前に、CCIの状態を更新 (例えばCopy One Generation から No More Copy) し、またブロックキー (Block Key) を生成する際に、ブロックシード (Block Seed) にDVR-EMIとして更新後のCCIの値を用いる場合には、コンテンツを受信するDVR側でコンテンツ受信後に、CCIの更新をせずに記録しても、DVR-EMIとコンテンツ中に埋めこまれているCCIが一致するので、記録モードはデータ解析記録方式 (Cognizant Mode) とする。これ以外の場合 (たとえば、コンテンツに埋めこむCCIの更新は行わないが、DVR-EMIは記録媒体上に記録された後の状態を表すようにする場合) は、記録モードはデータ非解析記録方式 (Non-Cognizant Mode) とする。

【0370】ステップS6102では、配信すべきコン

テンツデータの被暗号化データをTSパケットの形で受信する。なお、コンテンツ入力先は、予めコンテンツを格納したデータベース、あるいは別のコンテンツ提供サーバなどである。S6103で、各TSパケットを受信した時刻情報であるATS、およびコピー制御情報としてのCCIを付加する。次に、S6104で、ATSを付加したTSパケットを順次受信し、1ブロックを形成する例えばX=32に達したか、あるいはパケットの終了を示す識別データを受信したかを判定する。いずれかの条件が満足された場合はステップS6105に進み、X個、あるいはパケット終了までのパケットを並べて、1ブロックのブロックデータを形成する。

【0371】次に、S6106で、ブロックデータの先頭の32ビット (ATSを含むブロック・シード) とS6101で生成したタイトル固有キーとから、そのブロックのデータを暗号化する鍵であるブロックキーを生成する。

【0372】S6107では、ブロックキーを用いてブロックデータを暗号化して、記憶手段に記憶する。なお、先にも説明したように、暗号化の対象となるのは、ブロックデータのm+1バイト目から最終データまでである。暗号化アルゴリズムは、たとえばFIPS 46-2で規定されるDES (Data Encryption Standard) が適用される。

【0373】S6108で、全データを記録したかを判断する。全データを記録していれば、記録処理を終了し、全データを記録していなければS6102に戻って残りのデータの処理を実行する。

【0374】次に、(b) 暗号化コンテンツデータ送信処理について説明する。ステップS6121では、暗号化コンテンツを記憶手段から読み出して送信し、S6122で全ブロックの読み出しが完了したか否かを判定する。送信されるコンテンツは、前述の(a) コンテンツの暗号化処理のステップS6101で生成したタイトル固有キーに基づいて生成されるブロックキーで暗号化処理されたデータである。

【0375】次に、(c) タイトル固有キー送信処理について説明する。ステップS6131では、送信機器 (ここではDVRシステム) と相互認証が実行される。明示的な認証および鍵交換 (Authentication and Key Exchange) のプロトコルとしては、先に、機器間のコンテンツコピー処理の項目で図49、図50を用いて説明した共通鍵暗号方式、公開鍵暗号方式による認証が可能である。なお、共通鍵暗号やそれに基づくハッシュ関数を用いた共通鍵ベースの認証方法は、サーバと受信機器の2つのデバイス間で同一の秘密を持っていることを確認するものであるが、2つのデバイス間に同一の秘密を持たせる方法としては、あらかじめシステム全体で共通の秘密 (Global Secret) を全機器に持たせておく方法や、前述のツリー構造による鍵配信構成により、各機器にデ

バイスキーを持たせておき、それを用いてEKB処理によってルートキーを取得する構成として、ルートキーをデバイス間の共通秘密とする方法や、サーバ以外のデバイスに個々に秘密鍵を割り当て、どの機器にどのような値の秘密鍵を割り当てたかをサーバで管理しておくという構成が可能である。

【0376】この方法を用いる場合、たとえば図49に示す相互認証プロトコルを開始する前に、DVR機器からその記録媒体上もしくは機器内に格納してあるEKBを伝送し、これに基づいてサーバとデバイスがそれぞれルートキーを計算して共通鍵に設定した後、プロトコルを開始する構成とする。公開鍵暗号技術を用いる相互認証は各デバイスに公開鍵と秘密鍵のペアを持たせて認証、鍵交換を行うものである。公開鍵技術を用いたシステムでは、デバイスキーが露呈した機器をシステムから排除するのに使用するリスト、すなわち、排除機器の公開鍵証明書リストとした公開鍵証明書排除リスト(CRL: Certificate Revocation List)を用いることが可能である。前述のツリー構造鍵配信構成を用いると、EKBをCRLとして使用することができ、一般的な、排除する機器のIDを並べるCRLに比べてサイズを小さくできる利点がある。

【0377】図59の(c)タイトル固有キー送信処理のステップS6131の相互認証の成立がS6132において判定され、認証が成立しない場合は、タイトル固有キーの送信処理が中止される。S6132において、相互認証が成立したと判定されると、ステップS6133において、前述の(a)コンテンツの暗号化処理のステップS6101において生成したタイトル固有キーと、決定した記録モードを、(c)タイトル固有キー送信処理のステップS6131の相互認証において取得したセッションキーを用いて暗号化して送信する。一方、暗号化コンテンツを受信し、格納する記録再生装置における処理について、図60、図61を参照して説明する。ここでは、コンテンツ受信機器がDVRシステムであると想定して説明する。図61の処理フローの各ステップについて説明する。図61には、前述のサーバ側処理として実行される(b)暗号化コンテンツデータ送信処理、(c)タイトル固有キー送信処理の各処理に対応するデータ受信側処理として(b')暗号化コンテンツデータ受信処理、(c')タイトル固有キー受信処理に分けて記載してある。

【0378】(b')暗号化コンテンツデータ受信処理では、ステップS6201で、暗号化ブロックデータを受信し、ディスクに格納し、ステップS6202で全データの受信完了を確認し終了する。ここで格納されるデータは、コンテンツ配信サーバが図59の(a)コンテンツの暗号化処理のステップS6101で生成したタイトル固有キーに基づいて生成されるブロックキーで暗号化処理されたデータであり、復号、再暗号化のなされて

いないデータである。

【0379】(c')タイトル固有キー受信処理について説明する。ステップS6301では、データ送信側であるサーバ間で実行される相互認証、鍵交換処理であり、図59の説明と同様の処理である。

【0380】相互認証が成立すると、コンテンツ受信機器であるDVRシステムは、ステップS6303において、記録再生装置自身のメモリに格納しているマスターキーおよびデータ解析記録方式用キー(Cognizant Key)(データ解析記録方式(Cognizant Mode)の場合)もしくはデータ非解析記録方式用キー(Non-Cognizant Key)(データ非解析記録方式(Non-Cognizant Mode)の場合)を読み出す。また、ディスクからスタンパーID(Stamper ID)を読み出す。

【0381】S6304において、記録媒体に識別情報としてのディスクID(Disc ID)が既に記録されているかどうかを検査する。記録されていればS6305でこのディスクIDを読み出し、記録されていなければS6306で、ランダムに、もしくはあらかじめ定められた方法でディスクIDを生成し、ディスクに記録する。次に、S6307では、マスターキーとスタンパーID(Stamper ID)とディスクIDを用いて、ディスク固有キーを生成する。ディスク固有キーは先に説明したように、例えば、FIPS 180-1で定められているハッシュ関数SHA-1を用いる方法やブロック暗号に基づくハッシュ関数を使用する方法などを適用することで求める。

【0382】次にS6308に進み、コンテンツ送信側機器から暗号化されたタイトル固有キーと、記録モードを受信して、先の認証処理において取得したセッションキーを用いて復号する。

【0383】次に、ステップS6309において、タイトルキーの生成処理を実行し、記録モードと共にディスク1620(図60参照)に格納する。タイトルキーの生成処理は、先の機器間のコンテンツコピーの項目で図51を参照して説明したと同様であり、図51に示すように、図22例1で説明したタイトル固有キーの生成処理の逆方向の処理として実行される。すなわち、コンテンツ送信機器から受信したタイトル固有キーを、ディスク固有キーを用いて64bitブロック暗号関数の逆関数により復号し、これをデータ解析記録方式用キー(Cognizant Key)(データ解析記録方式(Cognizant Mode)の場合)もしくはデータ非解析記録方式用キー(Non-Cognizant Key)(データ非解析記録方式(Non-Cognizant Mode)の場合)と排他論理和し、さらに、ディスク固有キーを用いて64bitブロック暗号関数の逆関数を適用して復号した結果としてタイトルキーを生成する。

【0384】ステップS6309では、上述の処理において、生成したタイトルキーを記録モードと共にディスクに格納し、処理を終了する。

【0385】上述の処理において、データ受信側機器で

あるDVRシステムは、データ送信側であるコンテンツ提供サーバにおいて生成したタイトル固有キーに基づいて生成されるブロックキーで暗号化したコンテンツを格納することになる。

【0386】しかし、暗号化コンテンツを受信して格納したDVRシステムは、コンテンツ提供サーバからタイトル固有キーを受信して、受信したタイトル固有キーに基づいて、タイトルキーを生成し、タイトルキーをディスクに格納する処理を実行しているの、先に説明した図22のタイトル固有キー生成処理を実行することで、サーバにおいて生成したと同じタイトル固有キーを生成することが可能となり、ディスクに格納した暗号化コンテンツの復号が可能となる。

【0387】上述のコンテンツ配信処理における、タイトル固有キーの配信処理は、サーバと受信機器との間で認証と鍵共有プロトコルを行い、正しい結果が得られたときのみ、サーバから受信機器にタイトル固有キーを暗号化して送信するものであった。これは、インターネットなどの双方向ネットワークを介して行う場合には都合がよいが、放送などの一方の伝送環境では行えない。

【0388】このような場合、暗示的な認証に基づいてタイトル固有キーを送信することが可能である。暗示的な認証とは、送るべきデータを暗号化して送信し、正しい受信機器のみがそれを復号してデータを得られることを期待するものである。先に図11等を用いて説明した方式はまさに暗示的な認証に基づく方式であり、正しく、しかもリボークされていないノードキーを持つデバイスだけがEKBからルートキーを計算することができる。すなわち、この方式のEKBに加えて、タイトル固有キーをルートキーで暗号化したデータをサーバが放送すれば、正しく、リボークされていないノードキーを持つ受信機器だけがEKBの復号により、ルートキーを計算でき、さらに取得したルートキーに基づいてタイトル固有キーを得ることが可能になる。

【0389】このようなEKBによるタイトル固有キーの配信を行なうことで、各デバイスとの相互認証を省略した処理について、図62を参照して説明する。図62は、タイトル固有キーをEKB配信するサーバの処理と、EKBによるタイトル固有キーを受信する記録再生装置の処理を示している。

【0390】サーバ側の処理について説明する。サーバは、ステップS6601において、前述の図11のツリー構造のリーフに相当し、正当なライセンスを保有する記録再生機器において復号処理可能なEKBを生成し、ステップS6602において、前述の図59の

(a) コンテンツの暗号化処理のステップS6101において生成したタイトル固有キーと、決定した記録モードを、EKBのルートキーで暗号化して、EKBとともに配信する。

【0391】EKBを受信する記録再生装置の処理につ

いて説明する。ステップS6801では、サーバからEKB、およびEKBのルートキーで暗号化したタイトル固有キーと、記録モードを受信する。ステップS6802では、自己の装置内に格納しているリーフキー、ノードキーを用いてEKB復号処理を実行し、ルートキーを取得する。ルートキーの取得できない場合は正当なライセンスを受けている機器ではないことになる。

【0392】次に、ステップS6803において、取得したルートキーを適用してルートキーで暗号化したタイトル固有キーと、記録モードの復号処理を行ない、タイトル固有キーと、記録モードを取得する。以下ステップS6804以下の処理は、図61(c')のステップS6303以下の処理と同様であるので説明を省略する。

【0393】このようにEKBを用いることにより、各デバイスとの相互認証を実行することなく、正当なライセンスを持つ機器に対してのみタイトル固有キーを配信することが可能となる。

【0394】なお、上述の例では、サーバからDVRへのコンテンツ配信処理について説明したが、その他の機器に対するコンテンツ配信処理も同様の考え方によって実行できる。すなわち、サーバからデータ受信側機器に暗号化コンテンツに対応するタイトル固有キーを入力して、データ受信側機器において、タイトル固有キーに基づいてタイトルキーを生成して、コンテンツに対応付けて記録媒体に格納する。

【0395】[9. 情報処理装置、サーバの構成] 上述した一連の処理を実行する記録再生装置またはサーバのハードウェア構成例について説明する。上述した各フロー、ブロック図を参照して説明した処理はハードウェア、ソフトウェアの組合わせにより実行可能である。例えば、記録再生装置、サーバにおける暗号処理手段は暗号化/復号LSIとして構成することも可能であるが、汎用のコンピュータや、1チップのマイクロコンピュータにプログラムを実行させることにより行う構成とすることができる。同様にTS処理手段も処理をソフトウェアによって実行することが可能である。一連の処理をソフトウェアによって行う場合には、そのソフトウェアを構成するプログラムが、汎用のコンピュータや1チップのマイクロコンピュータ等にインストールされる。図63は、上述した一連の処理を実行するプログラムがインストールされるコンピュータの一実施の形態の構成例を示している。

【0396】プログラムは、コンピュータに内蔵されている記録媒体としてのハードディスク4205やROM4203に予め記録しておくことができる。あるいは、プログラムはフロッピー（登録商標）ディスク、CD-ROM(Compact Disc Read Only Memory)、MO(Magneto optical)ディスク、DVD(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体4210に、一時的あるいは永続的に格納（記

録)しておくことができる。このようなリムーバブル記録媒体4210は、いわゆるパッケージソフトウェアとして提供することができる。

【0397】なお、プログラムは、上述したようなリムーバブル記録媒体4210からコンピュータにインストールする他、ダウンロードサイトから、デジタル衛星放送用の人工衛星を介して、コンピュータに無線で転送したり、LAN(Local AreaNetwork)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを、通信部4208で受信し、内蔵するハードディスク4205にインストールすることができる。

【0398】コンピュータは、CPU(Central Processing Unit)4202を内蔵している。CPU4202には、バス4201を介して、入出力インタフェース4211が接続されており、CPU4202は、入出力インタフェース4210を介して、ユーザによって、キーボードやマウス等で構成される入力部4207が操作されることにより指令が入力されると、それにしたがって、ROM(Read Only Memory)4203に格納されているプログラムを実行する。

【0399】あるいは、CPU4202は、ハードディスク4205に格納されているプログラム、衛星若しくはネットワークから転送され、通信部4208で受信されてハードディスク4205にインストールされたプログラム、またはドライブ4209に装着されたリムーバブル記録媒体4210から読み出されてハードディスク4205にインストールされたプログラムを、RAM(Random Access Memory)4204にロードして実行する。

【0400】これにより、CPU4202は、上述したフローチャートにしたがった処理、あるいは上述したブロック図の構成により行われる処理を行う。そして、CPU4202は、その処理結果を、必要に応じて、例えば、入出力インタフェース4211を介して、LCD(Liquid Crystal Display)やスピーカ等で構成される出力部4206から出力、あるいは、通信部4208から送信、さらには、ハードディスク4205に記録させる。

【0401】ここで、本明細書において、コンピュータに各種の処理を行わせるためのプログラムを記述する処理ステップは、必ずしもフローチャートとして記載された順序に沿って時系列に処理する必要はなく、並列的あるいは個別に実行される処理(例えば、並列処理あるいはオブジェクトによる処理)も含むものである。

【0402】また、プログラムは、1のコンピュータにより処理されるものであっても良いし、複数のコンピュータによって分散処理されるものであっても良い。さらに、プログラムは、遠方のコンピュータに転送されて実行されるものであっても良い。

【0403】なお、本実施の形態では、コンテンツの暗

号化/復号を行うブロックを、1チップの暗号化/復号LSIで構成する例を中心として説明したが、コンテンツの暗号化/復号を行うブロックは、例えば、図1および図2に示すCPU170が実行する1つのソフトウェアモジュールとして実現することも可能である。同様に、TS処理手段300の処理もCPU170が実行する1つのソフトウェアモジュールとして実現することが可能である。

【0404】以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。実施例においては、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【0405】

【発明の効果】上述したように、本発明の構成においては、コンテンツを情報記録再生装置間においてコピーまたは移動する際、あるいは配信コンテンツを情報記録再生装置の記録媒体に格納する際、コンテンツの再暗号化処理を実行せずに新たな記憶媒体に格納することが可能となるので、処理効率が高められる。

【0406】さらに、本発明の構成によれば、異なる情報記録再生装置においてデータをコピーまたは移動際、データ送信側の情報処理装置の生成したタイトル固有キーを入力して、データ受信側の情報処理装置においてタイトル固有キーに基づいてタイトルキーを生成して記録媒体に格納する構成とし、格納したタイトルキーに基づいて受信側の情報処理装置におけるタイトル固有キー生成シーケンスに従って生成されるタイトル固有キーを適用して格納コンテンツの再生を可能としたので、コンテンツの再暗号化を行わずに、ライセンスのある機器においてのみ再生可能なコンテンツとしたコピー処理構成が実現される。

【0407】さらに、本発明の構成によれば、コンテンツ提供サーバから配信されるコンテンツを情報記録再生装置に格納する際、サーバの生成したタイトル固有キーを入力して、データ受信側の情報処理装置においてタイトル固有キーに基づいてタイトルキーを生成して記録媒体に格納する構成とし、格納したタイトルキーに基づいて受信側の情報処理装置におけるタイトル固有キー生成シーケンスに従って生成されるタイトル固有キーを適用して格納コンテンツの再生を可能としたので、コンテンツの再暗号化を行わずに、ライセンスのある機器においてのみ再生可能なコンテンツとするデータ格納処理構成が実現される。

【0408】また、本発明の構成によれば、ツリー

(木)構造の鍵配布構成により、タイトル固有キーを有効化キーブロック(EKB)とともに送信し、送信した

EKBの処理によりタイトル固有キーを取得する構成としたので、機器毎の相互認証を実行せずに、ライセンスを有する機器に対してタイトル固有キーを確実に配信することが可能となる。

【図面の簡単な説明】

【図1】本発明の情報処理装置の構成例（その1）を示すブロック図である。

【図2】本発明の情報処理装置の構成例（その2）を示すブロック図である。

【図3】本発明の情報処理装置のデータ記録処理フローを示す図である。

【図4】本発明の情報処理装置のデータ再生処理フローを示す図である。

【図5】本発明の情報処理装置において処理されるデータフォーマットを説明する図である。

【図6】本発明の情報処理装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図7】本発明の情報処理装置において処理されるトランスポート・ストリームの構成を説明する図である。

【図8】本発明の情報処理装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図9】本発明の情報処理装置におけるトランスポート・ストリーム（TS）処理手段の構成を示すブロック図である。

【図10】本発明の情報処理装置において処理されるブロックデータの付加情報としてのブロック・データの構成例を示す図である。

【図11】本発明の情報処理装置に対するマスターキー、メディアキー等の鍵の暗号化処理について説明するツリー構成図である。

【図12】本発明の情報処理装置に対するマスターキー、メディアキー等の鍵の配布に使用される有効化キーブロック（EKB）の例を示す図である。

【図13】本発明の情報処理装置におけるマスターキーの有効化キーブロック（EKB）を使用した配布例と復号処理例を示す図である。

【図14】本発明の情報処理装置におけるマスターキーの有効化キーブロック（EKB）を使用した復号処理フローを示す図である。

【図15】本発明の情報処理装置におけるコンテンツ記録処理におけるマスターキーの世代比較処理フローを示す図である。

【図16】本発明の情報処理装置において、データ記録処理時の暗号化処理を説明するブロック図（その1）である。

【図17】本発明の情報処理装置において、データ記録処理時の暗号化処理を説明するブロック図（その2）である。

【図18】本発明の情報処理装置において、データ記録処理を説明するフローチャートである。

【図19】本発明の情報処理装置におけるディスク固有キーの生成例を説明する図である。

【図20】本発明の情報処理装置において処理される伝送1394パケットにおけるEMI格納位置（5CDT C P規格）を示す図である。

【図21】本発明の情報処理装置におけるコンテンツ記録をデータ解析記録方式（Cognizant Mode）によって実行するか、データ非解析記録方式（Non-Cognizant Mode）で実行するかを決定するプロセスを説明するフロー図である。

【図22】本発明の情報処理装置において、データ記録時のタイトル固有キーの生成処理例を示す図である。

【図23】本発明の情報処理装置におけるブロック・キーの生成方法を説明する図である。

【図24】本発明の情報処理装置におけるタイトル固有キーの生成処理フローを示す図である。

【図25】本発明の情報処理装置において、データ再生処理時のコンテンツデータ復号処理を説明するブロック図である。

【図26】本発明の情報処理装置において、データ再生処理を説明するフローチャートである。

【図27】本発明の情報処理装置において、データ再生処理における再生可能制判定処理の詳細を示すフローチャートである。

【図28】本発明の情報処理装置において、データ再生時のタイトル固有キーの生成処理フローを示す図である。

【図29】本発明の情報処理装置におけるメディアキーの有効化キーブロック（EKB）を使用した配布例と復号処理例を示す図である。

【図30】本発明の情報処理装置におけるメディアキーの有効化キーブロック（EKB）を使用した復号処理フローを示す図である。

【図31】本発明の情報処理装置におけるメディアキーを使用したコンテンツ記録処理フローを示す図である。

【図32】本発明の情報処理装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その1）である。

【図33】本発明の情報処理装置において、メディアキーを使用したデータ記録処理時の暗号化処理を説明するブロック図（その2）である。

【図34】本発明の情報処理装置において、メディアキーを使用したデータ記録処理を説明するフローチャートである。

【図35】本発明の情報処理装置において、メディアキーを使用したデータ再生処理時の暗号化処理を説明するブロック図である。

【図36】本発明の情報処理装置において、メディアキ

ーを使用したデータ再生処理を説明するフローチャートである。

【図37】本発明の情報処理装置において、メディアキーを使用したデータ再生処理における再生可能性判定処理の詳細を示すフローチャートである。

【図38】本発明の情報処理装置において、LSIキーを使用したデータ記録処理時の暗号化処理を説明するブロック図である。

【図39】本発明の情報処理装置において、LSIキーを使用したデータ記録処理の詳細を示すフローチャートである。

【図40】本発明の情報処理装置において、LSIキーを使用したタイトル固有キーの生成処理構成を説明する図である。

【図41】本発明の情報処理装置において、LSIキーを使用したデータ再生処理時の暗号処理を説明するブロック図である。

【図42】本発明の情報処理装置において、LSIキーを使用したデータ再生処理の詳細を示すフローチャートである。

【図43】本発明の情報処理装置におけるデータ記録処理時のコピー制御処理を説明するフローチャートである。

【図44】本発明の情報処理装置におけるデータ再生処理時のコピー制御処理を説明するフローチャートである。

【図45】情報処理装置間のデータコピー処理におけるデータ送信側機器（HDR）の処理を説明するブロック図である。

【図46】情報処理装置間のデータコピー処理におけるデータ送信側機器（HDR）の処理を説明するフロー図である。

【図47】情報処理装置間のデータコピー処理におけるデータ受信側機器（DVR）の処理を説明するブロック図である。

【図48】情報処理装置間のデータコピー処理におけるデータ受信側機器（DVR）の処理を説明するフロー図である。

【図49】MAC値を用いた相互認証処理を説明する図である。

【図50】公開鍵暗号方式の相互認証処理を説明する図である。

【図51】タイトル固有キーからタイトルキーの生成を実行する処理構成を説明する図である。

【図52】タイトル固有キー等におけるデータ縮約、伸長処理構成を説明する図である。

【図53】情報処理装置間のデータコピー処理におけるデータ送信側機器（DVR）の処理を説明するブロック図である。

【図54】情報処理装置間のデータコピー処理における

データ送信側機器（DVR）の処理を説明するフロー図である。

【図55】情報処理装置間のデータコピー処理におけるデータ受信側機器（HDR）の処理を説明するブロック図である。

【図56】情報処理装置間のデータコピー処理におけるデータ受信側機器（HDR）の処理を説明するフロー図である。

【図57】タイトル固有キーからタイトルキーの生成を実行する処理構成を説明する図である。

【図58】データ配信処理におけるサーバの処理を説明するブロック図である。

【図59】データ配信処理におけるサーバの処理を説明するフロー図である。

【図60】データ配信処理におけるデータ受信側機器（DVR）の処理を説明するブロック図である。

【図61】データ配信処理におけるデータ受信側機器（DVR）の処理を説明するフロー図である。

【図62】データ配信処理におけるEKBによるタイトル固有キーの送受信処理を説明するフロー図である。

【図63】情報記録再生装置、サーバの処理手段構成を示したブロック図である。

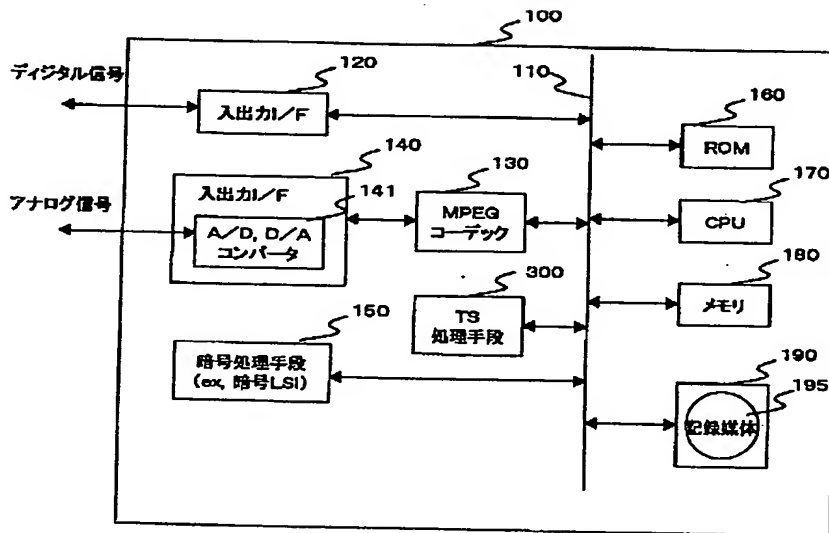
【符号の説明】

100, 200	記録再生装置
110	バス
120	入出力I/F
130	MPEGコーデック
140	入出力I/F
141	A/D, D/Aコンバータ
150	暗号処理手段
160	ROM
170	CPU
180	メモリ
190	ドライブ
195	記録媒体
210	記録媒体I/F
300	TS処理手段
600, 607	端子
602	ビットストリームパーサー
603	PLL
604	タイムスタンプ発生回路
605	ブロックシード付加回路
606	スムージングバッファ
800, 806	端子
801	ブロックシード分離回路
802	出力制御回路
803	比較器
804	タイミング発生回路
805	27MHzクロック
901, 904, 913	端子

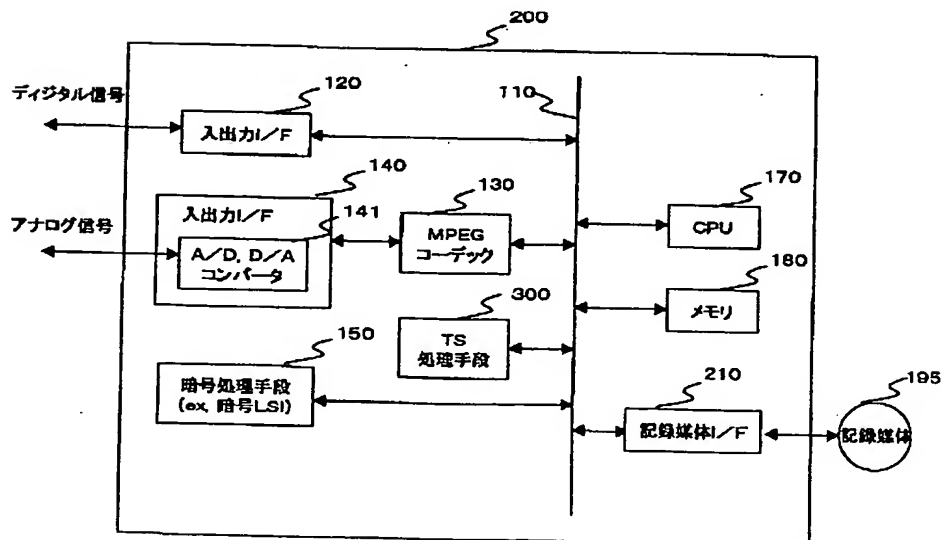
902 MPEGビデオエンコーダ
 903 ビデオストリームバッファ
 905 MPEGオーディオエンコーダ
 906 オーディオストリームバッファ
 908 多重化スケジューラ
 909 トランスポートパケット符号化器
 910 到着タイムスタンプ計算手段
 911 ブロックシード付加回路
 912 スムージングバッファ
 976 スイッチ

4202 CPU
 4203 ROM
 4204 RAM
 4205 ハードディスク
 4206 出力部
 4207 入力部
 4208 通信部
 4209 ドライブ
 4210 リムーバブル記録媒体
 4211 入出力インタフェース

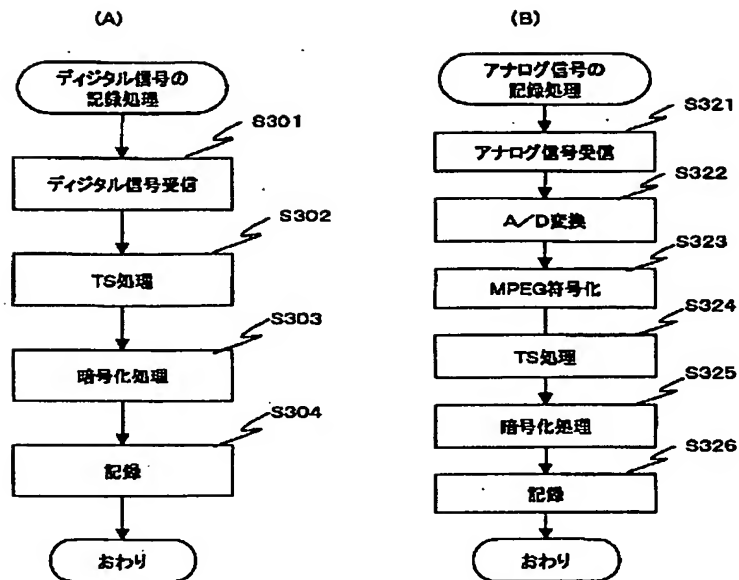
【図1】



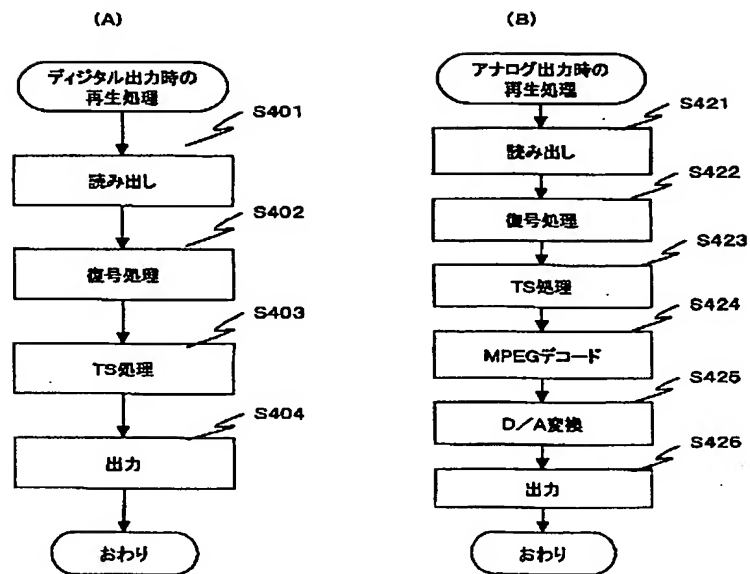
【図2】



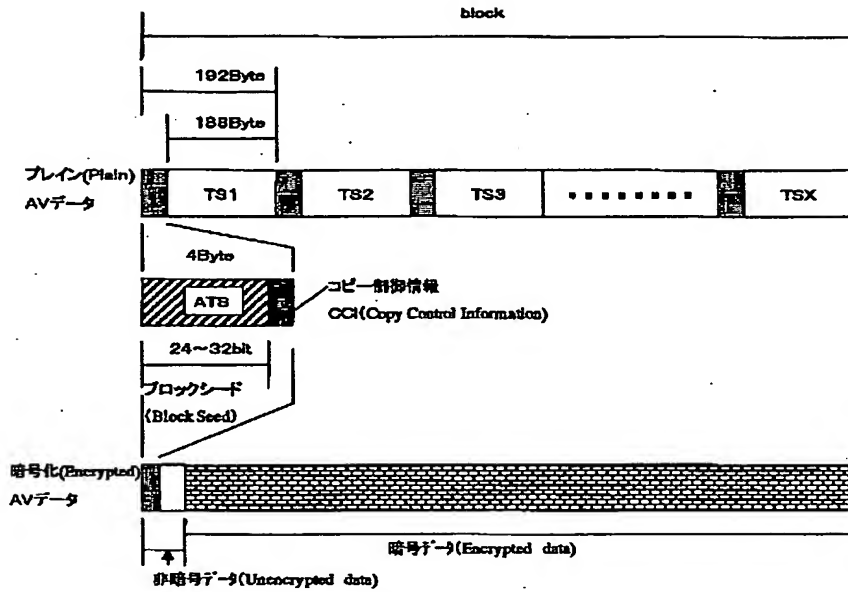
【図3】



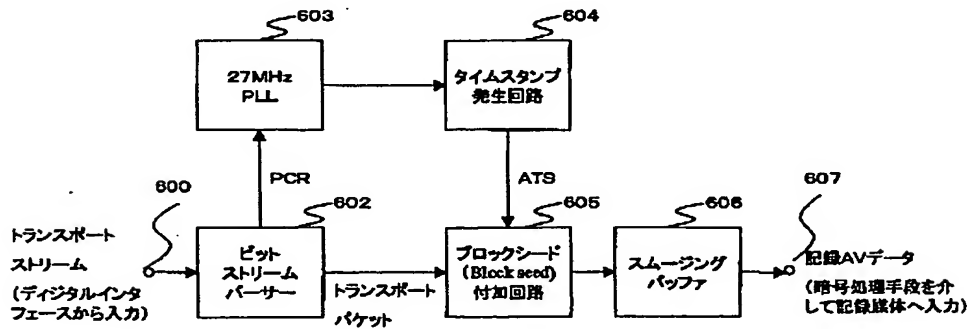
【図4】



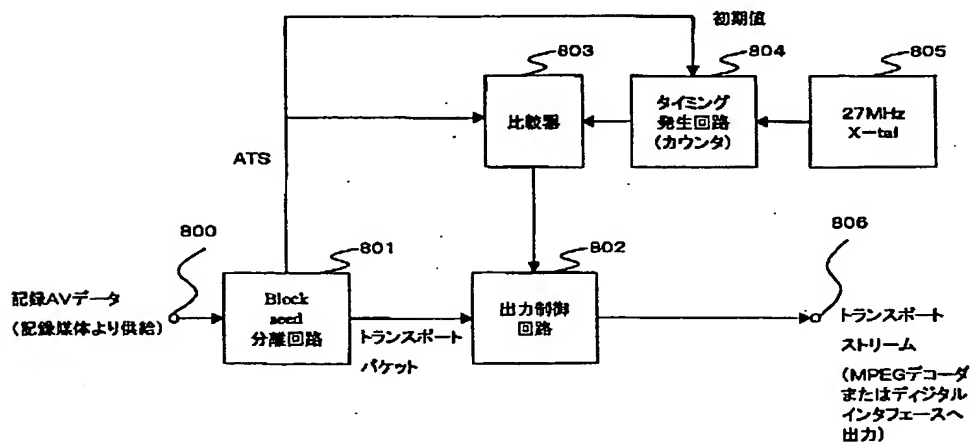
【図5】



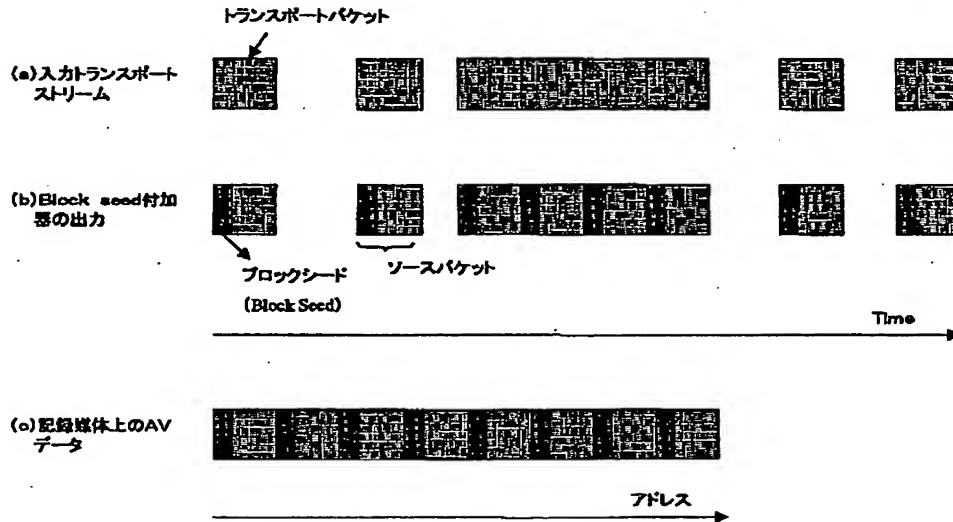
【図6】



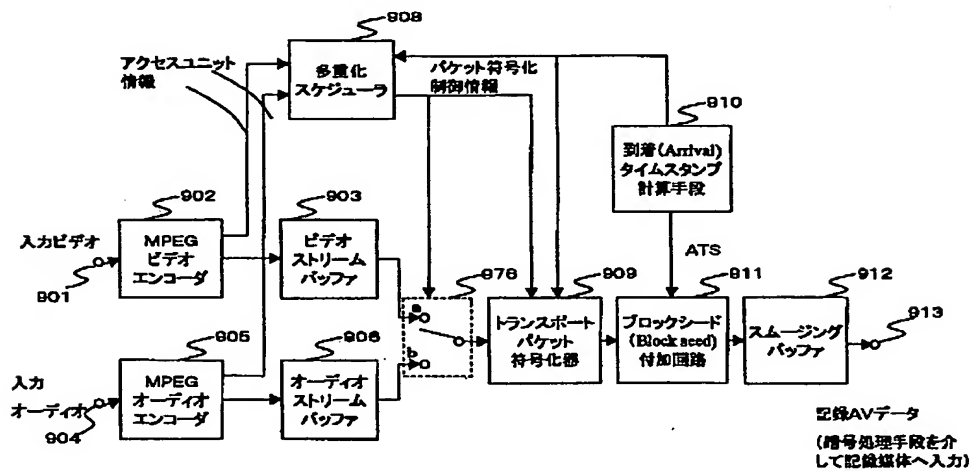
【図8】



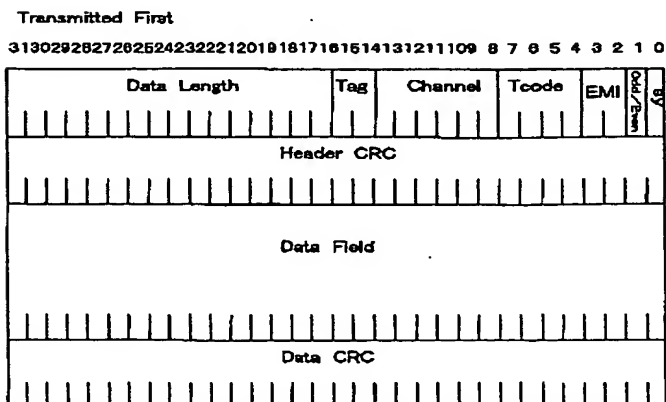
【図7】



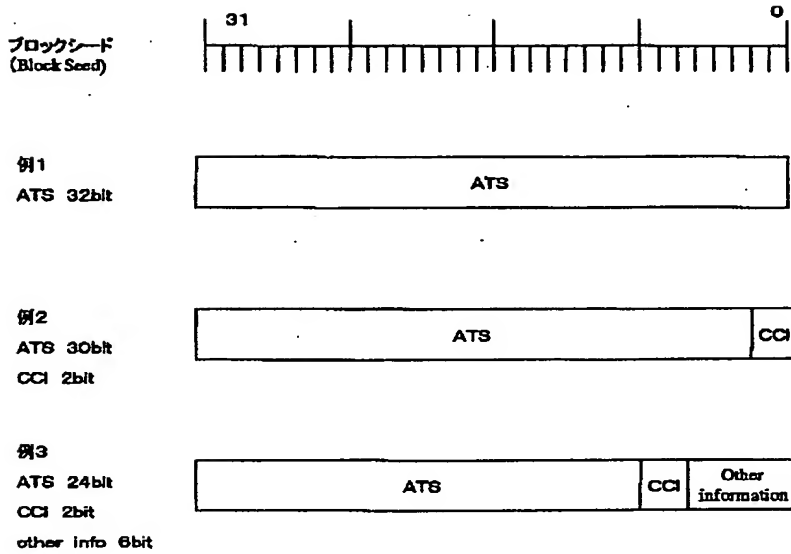
【図9】



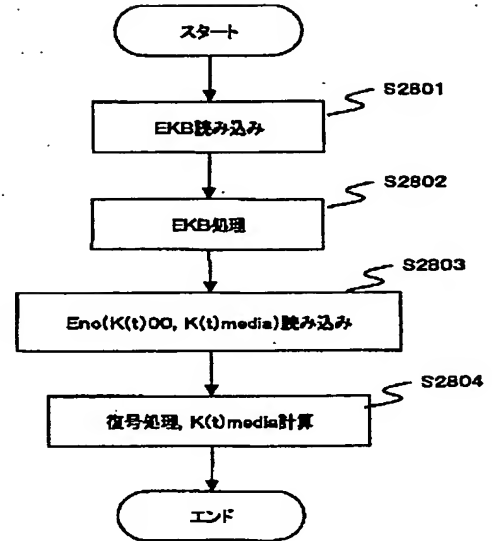
【図20】



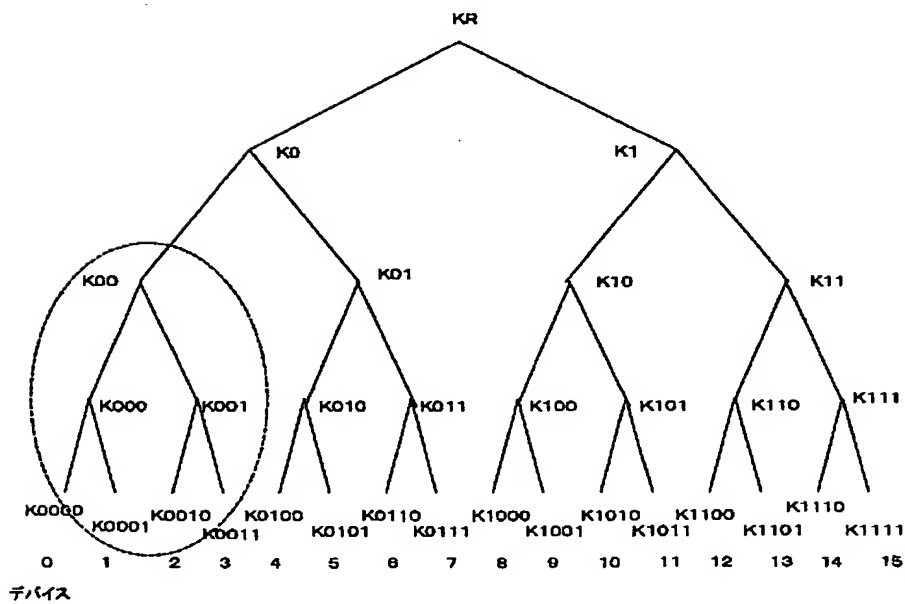
【図10】



【図30】



【図11】



【図12】

(A) キー更新ブロック(KRB:Key Renewal Block) 例1

デバイス0, 1, 2に時点でのルートキー $K(t)R$ を送付

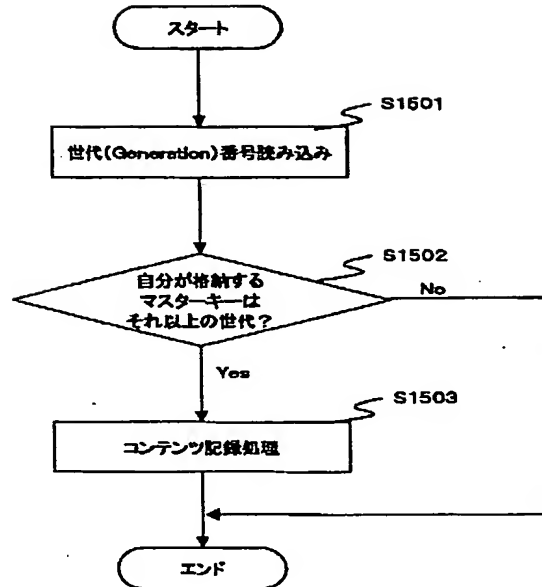
世代(Generation):t	
インデックス	暗号化キー
0	$Enc(K(t)0, K(t)R)$
00	$Enc(K(t)00, K(t)0)$
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

(B) キー更新ブロック(KRB:Key Renewal Block) 例2

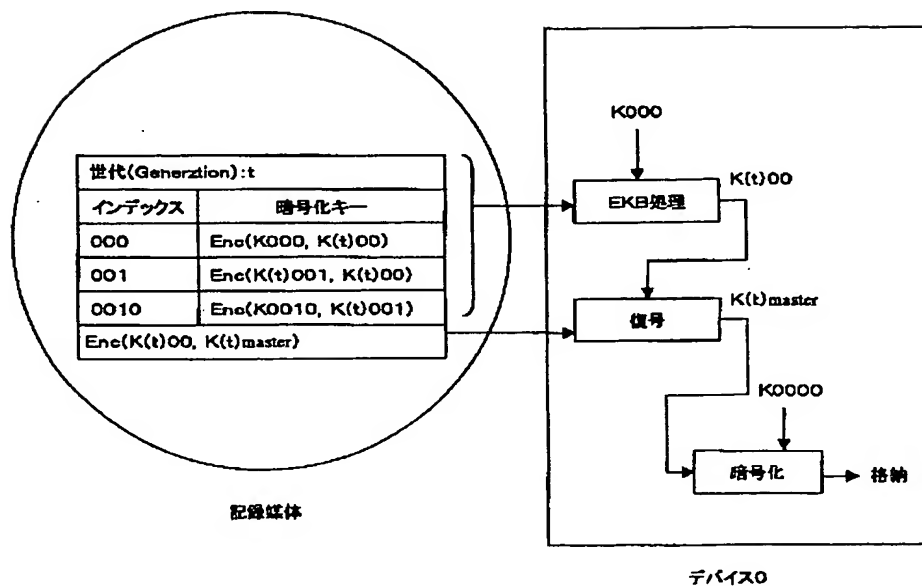
デバイス0, 1, 2に時点でのルートキー $K(t)R$ を送付

世代(Generation):t	
インデックス	暗号化キー
000	$Enc(K000, K(t)00)$
001	$Enc(K(t)001, K(t)00)$
0010	$Enc(K0010, K(t)001)$

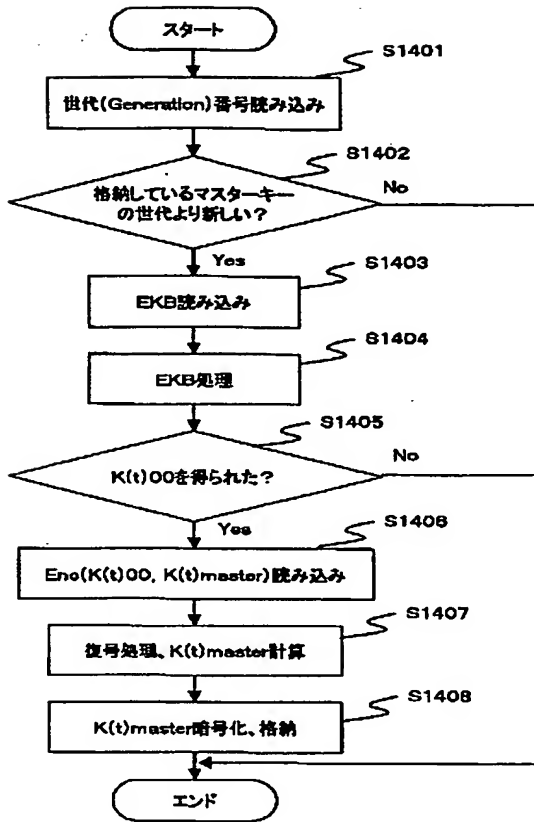
【図15】



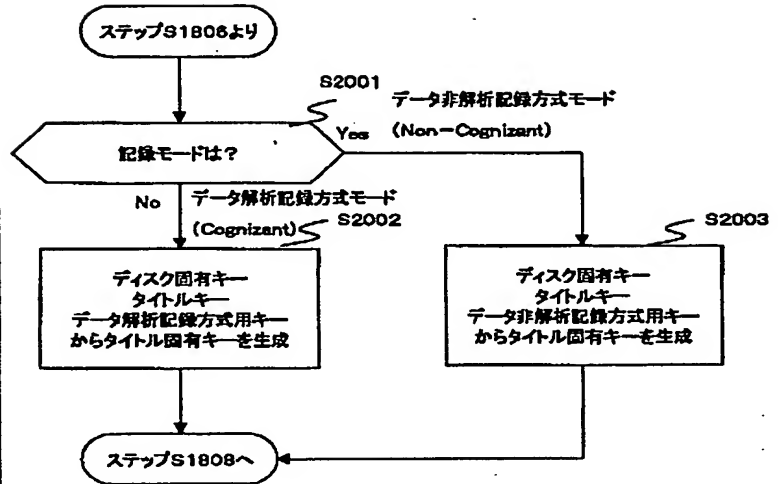
【図13】



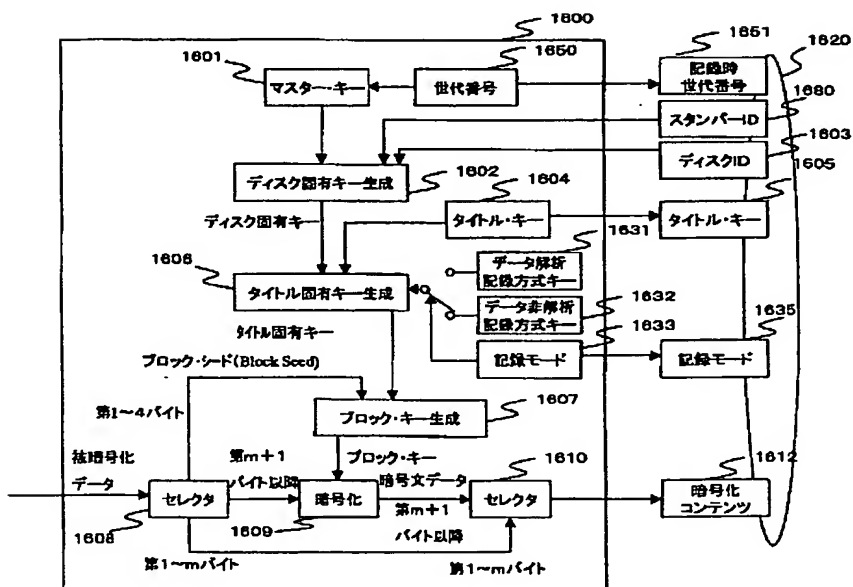
【図14】



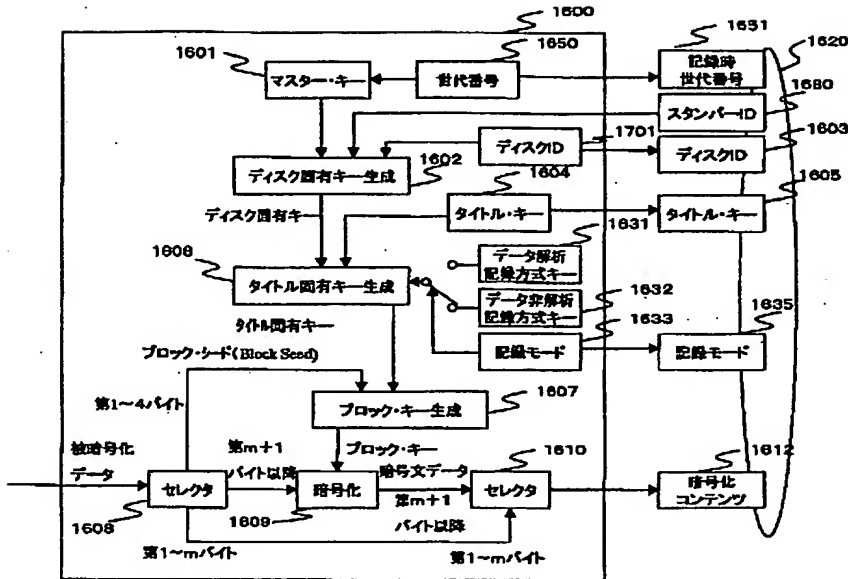
【図24】



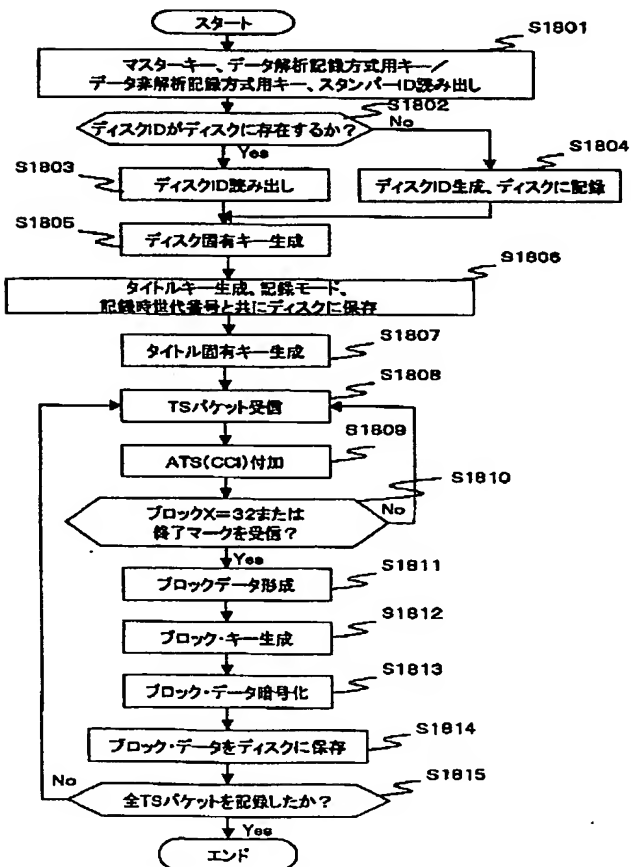
【図16】



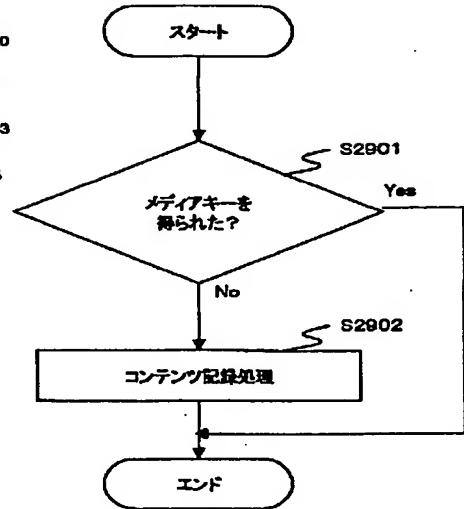
【図17】



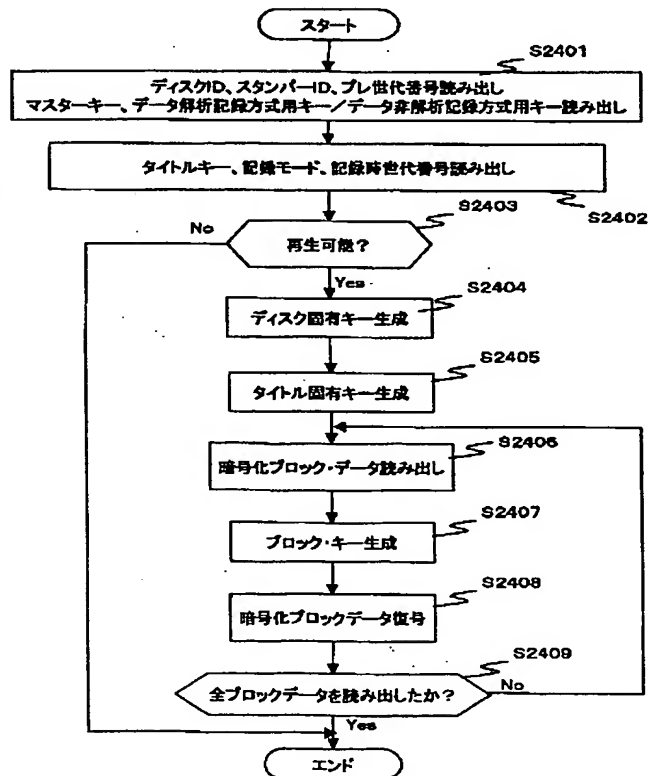
【図18】



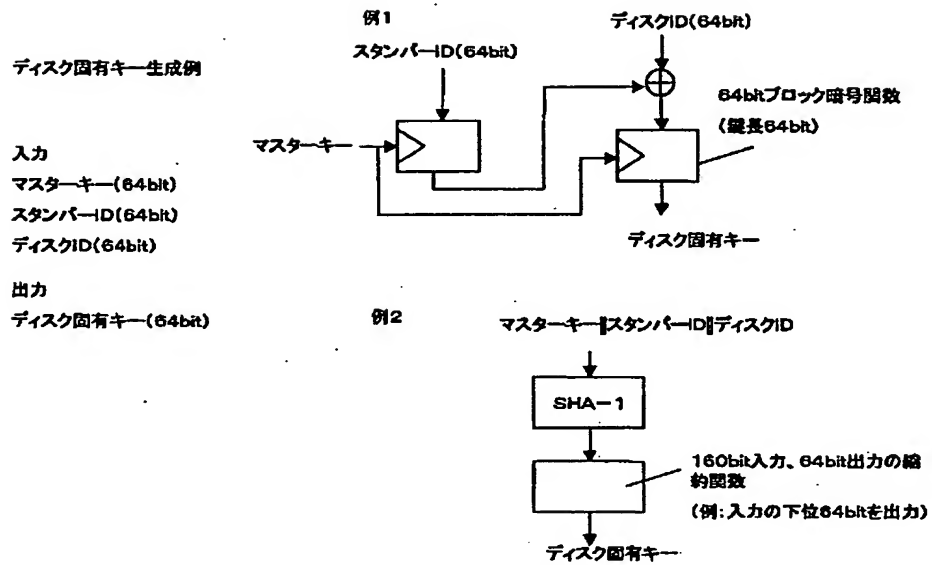
【図31】



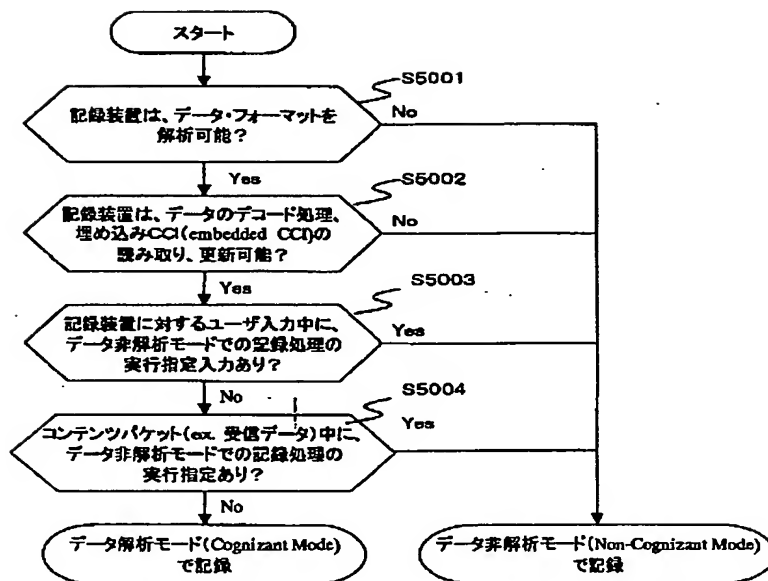
【図26】



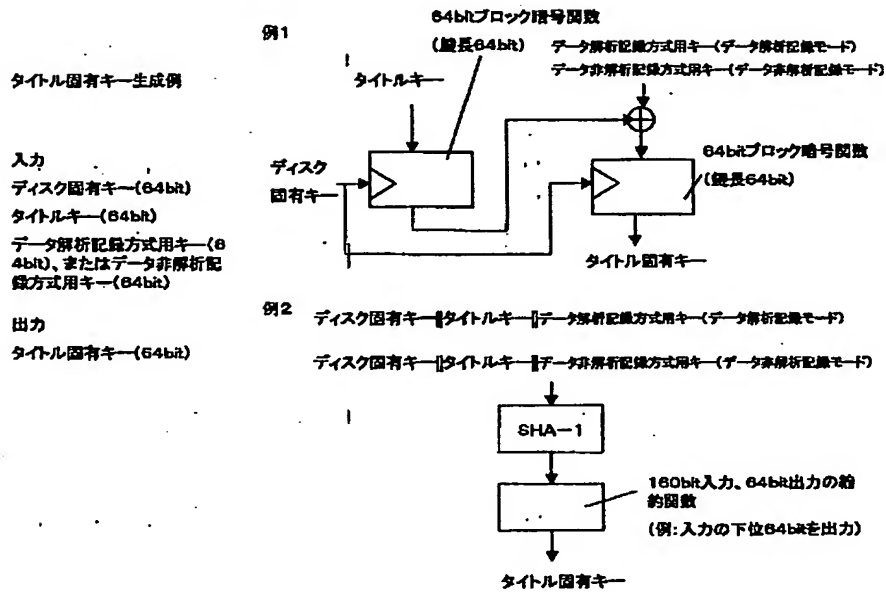
【図19】



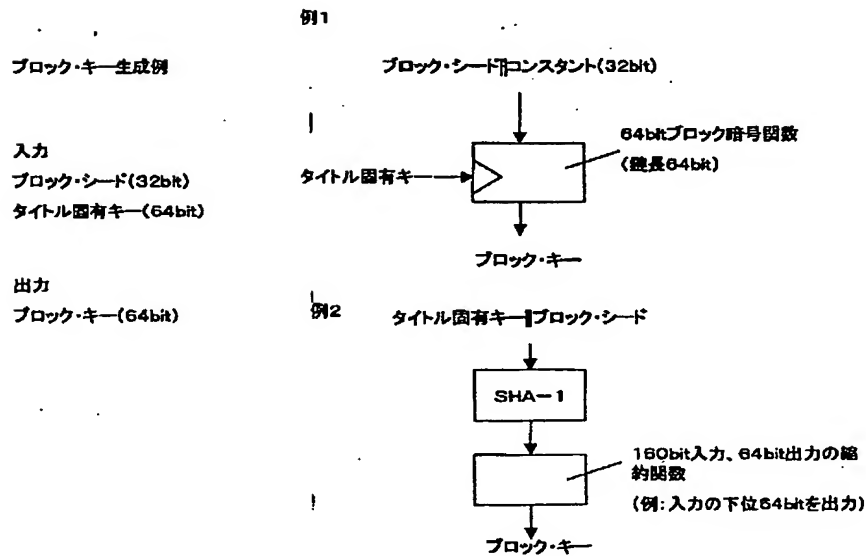
【図21】



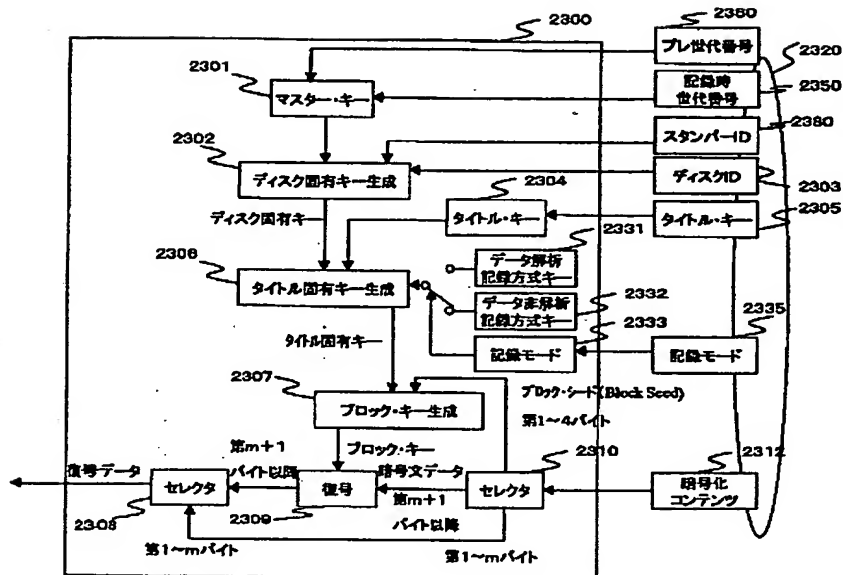
【図22】



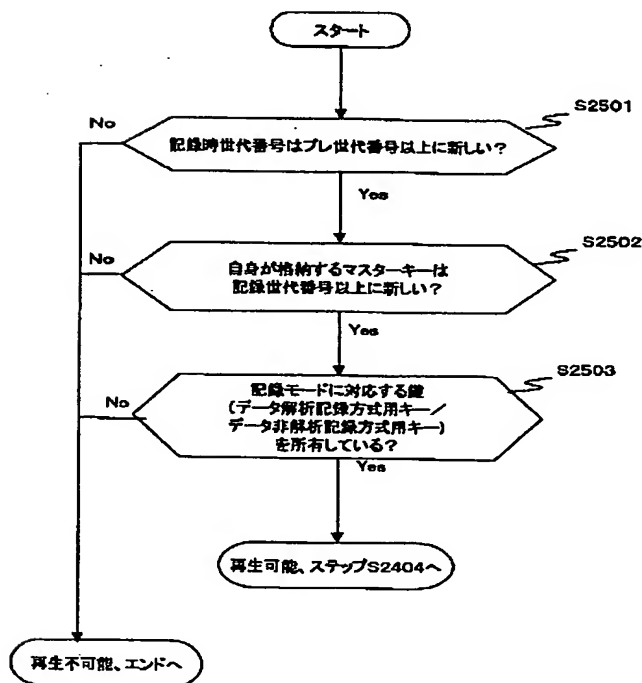
【図23】



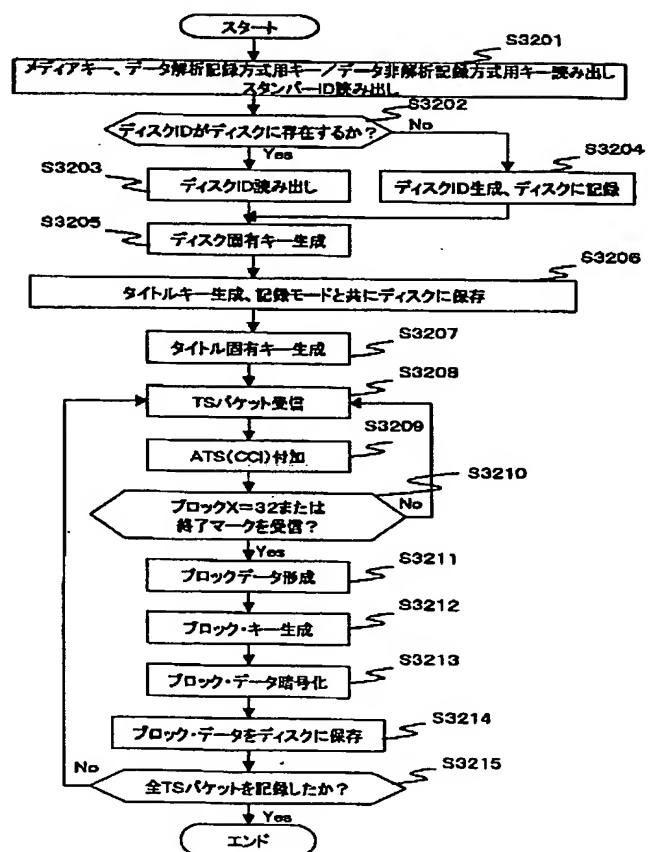
【図25】



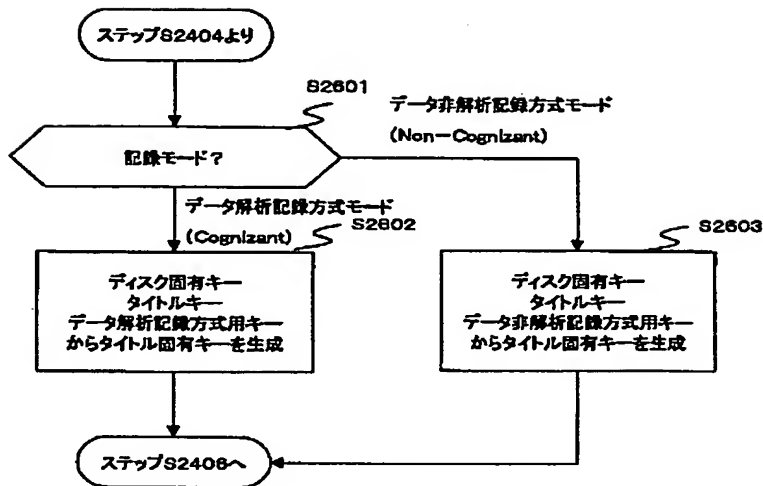
【図27】



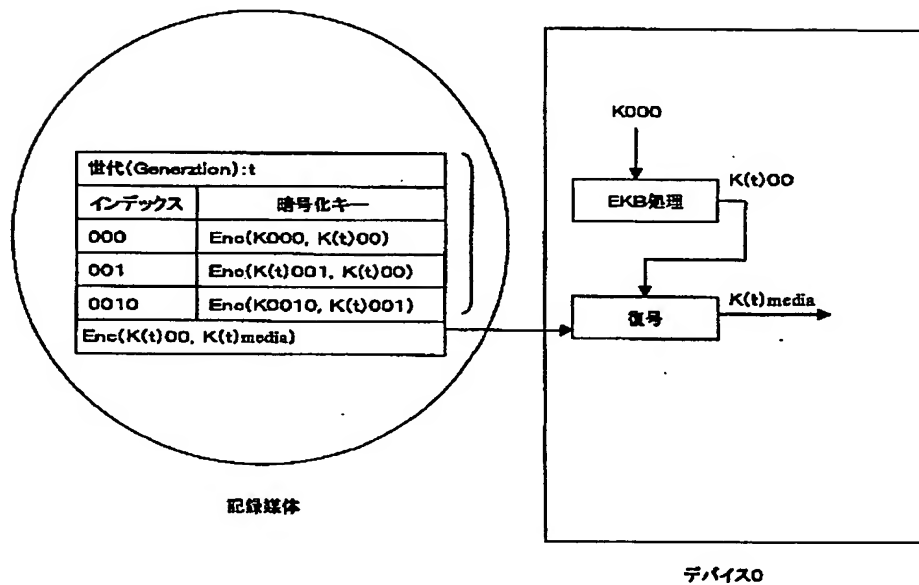
【図34】



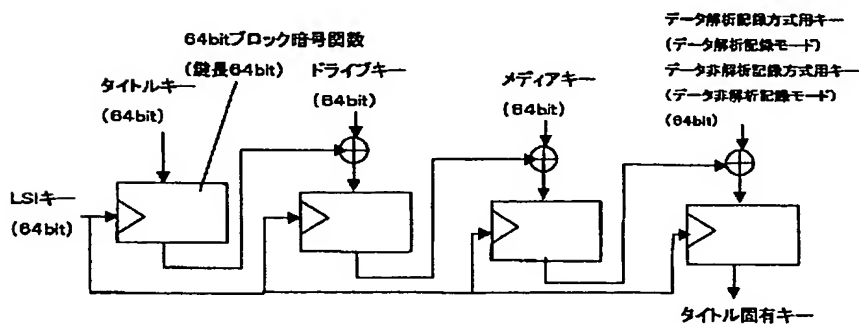
【図28】



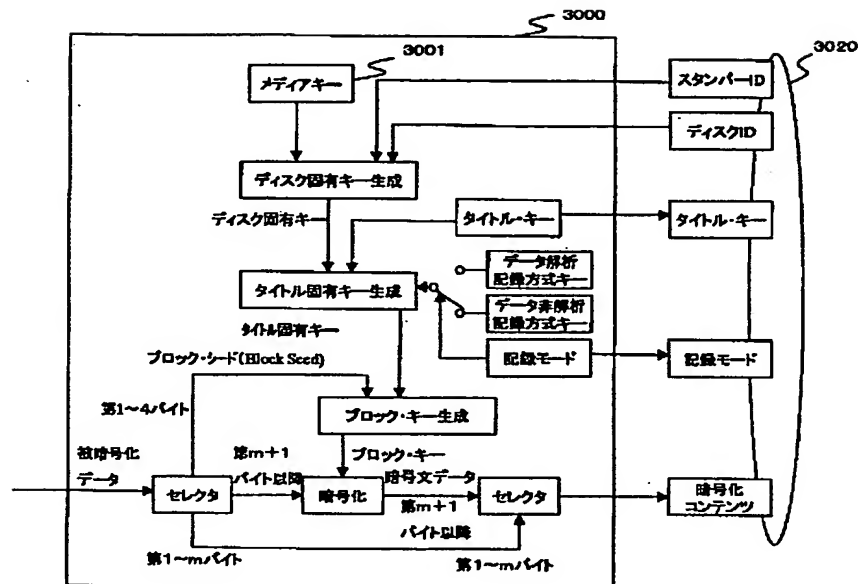
【図29】



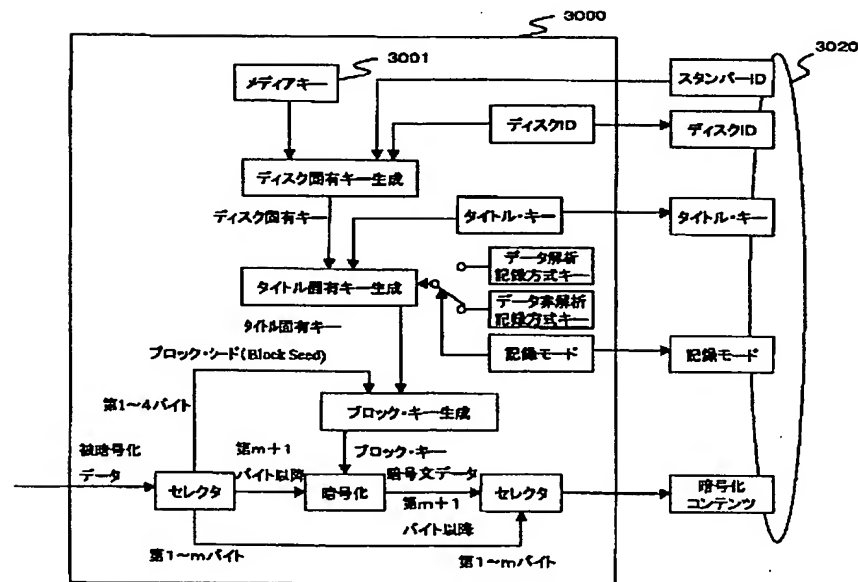
【図40】



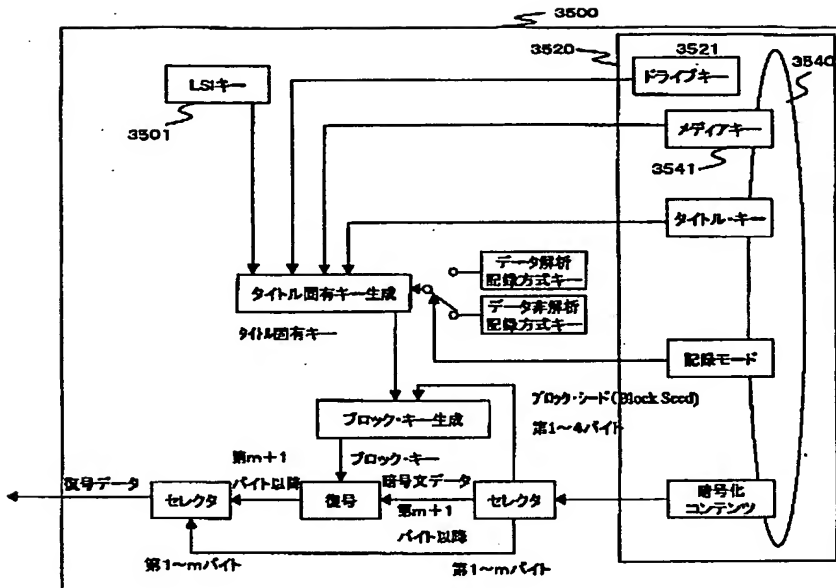
【図32】



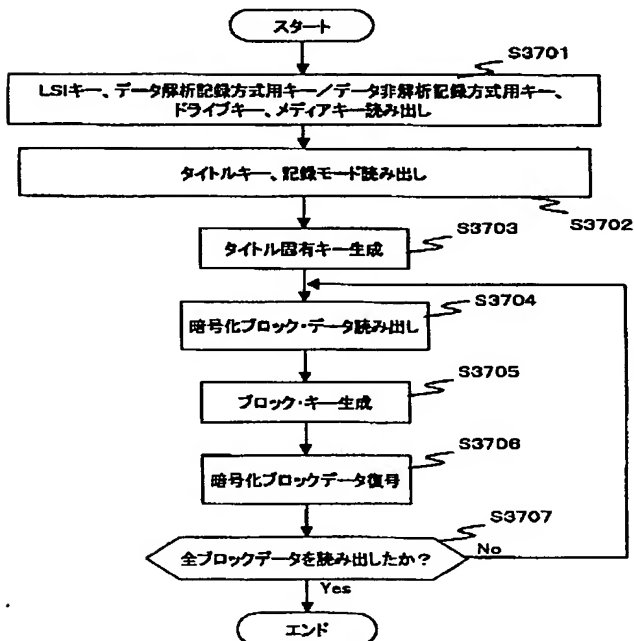
【図33】



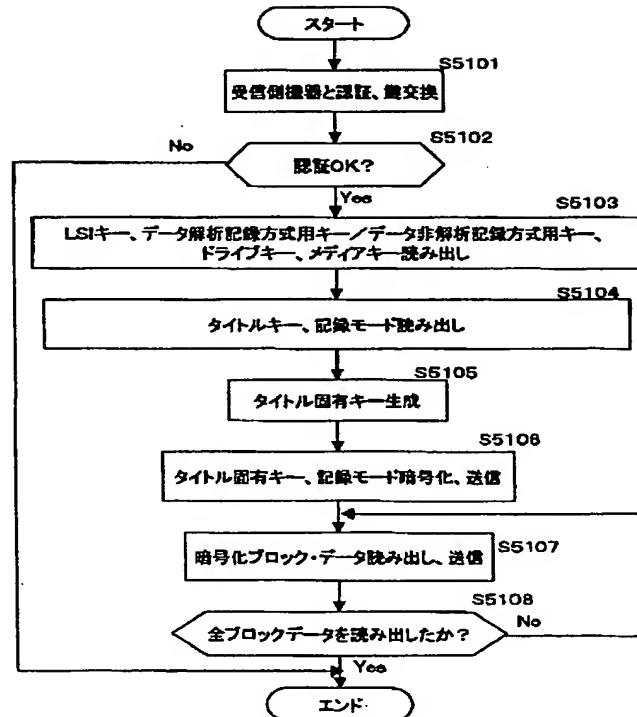
【図41】



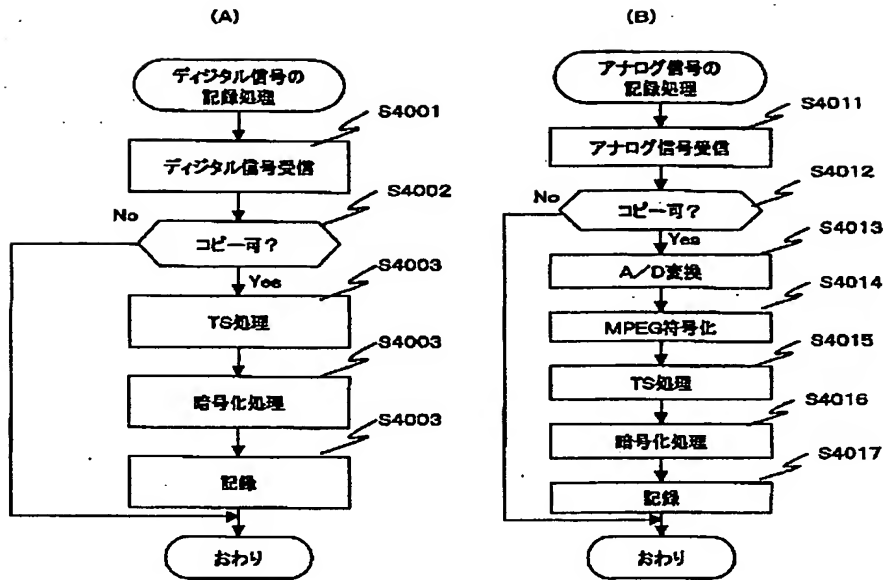
【図42】



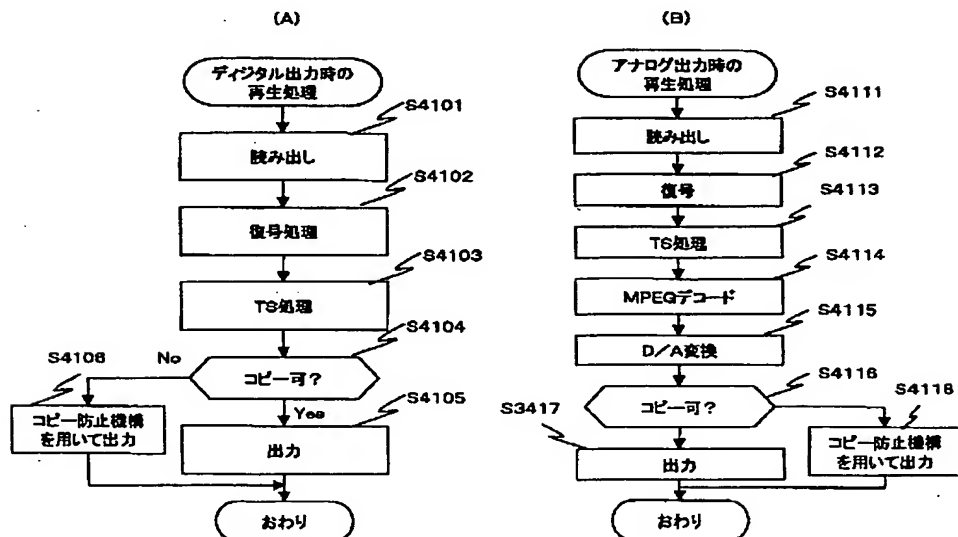
【図46】



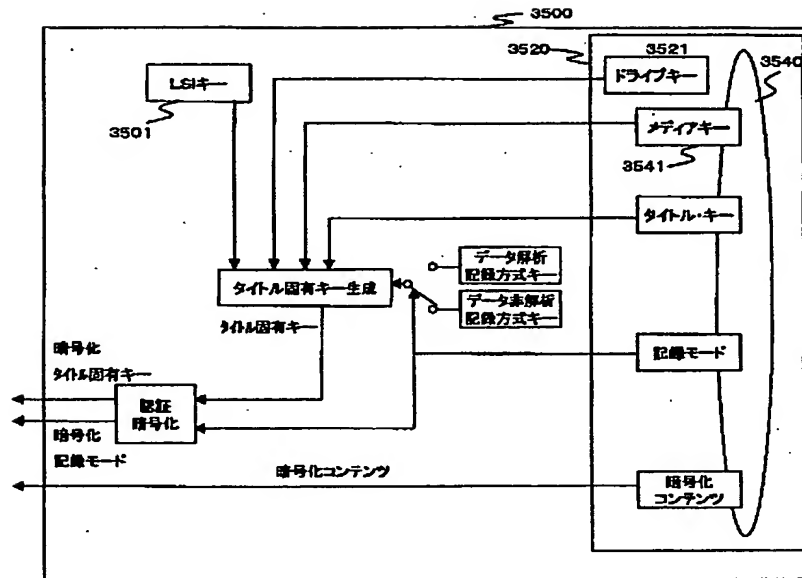
【図43】



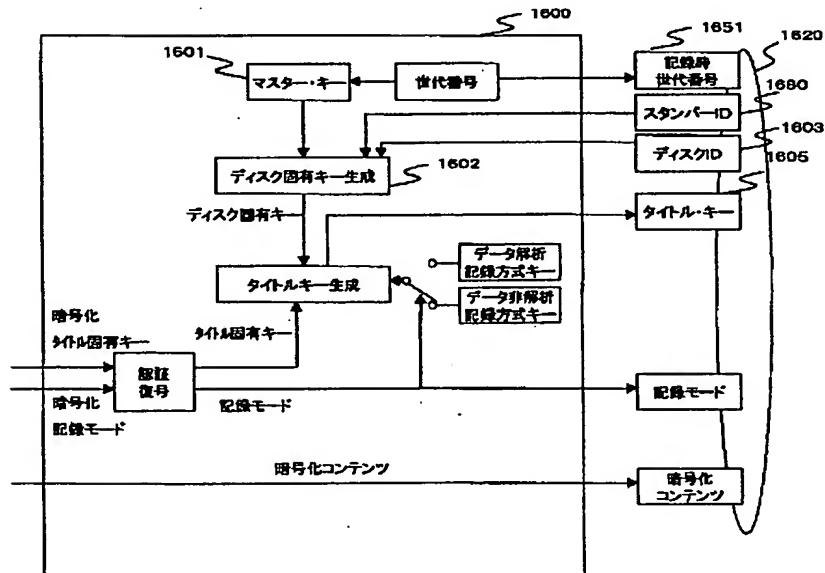
【図44】



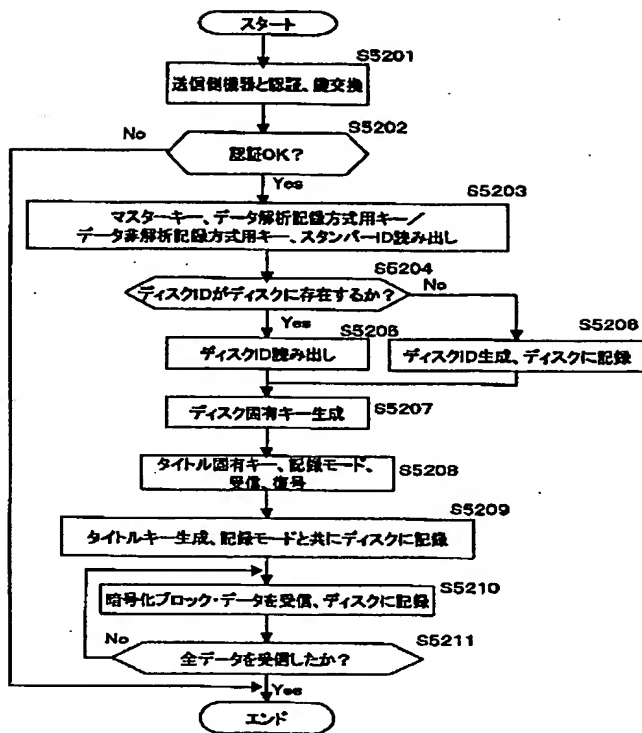
【図45】



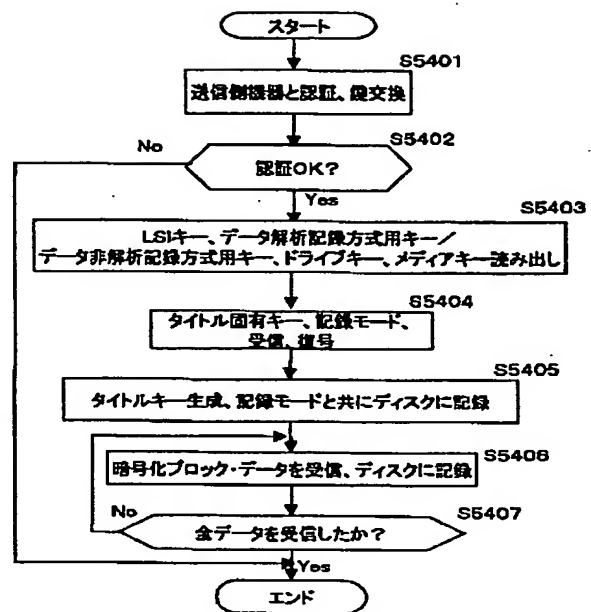
【図47】



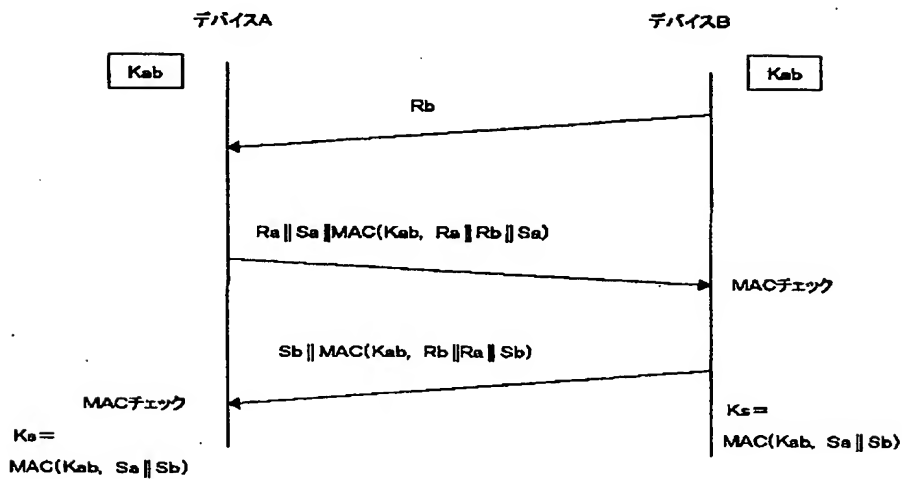
【図48】



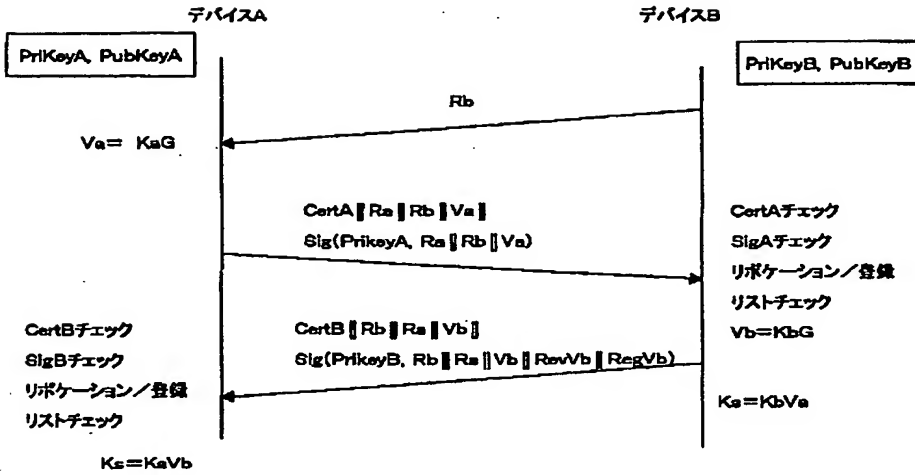
【図56】



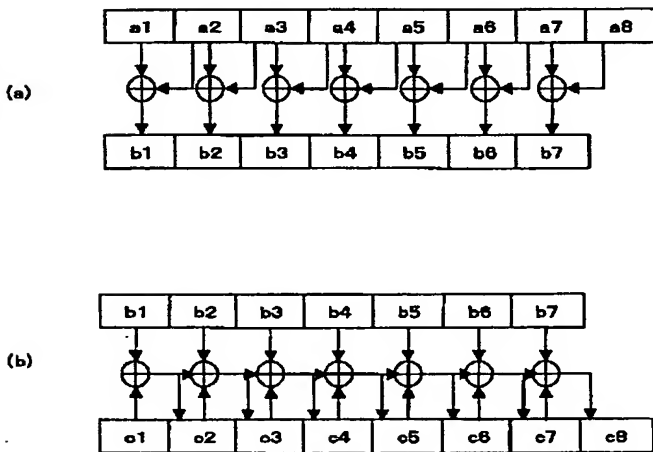
【図49】



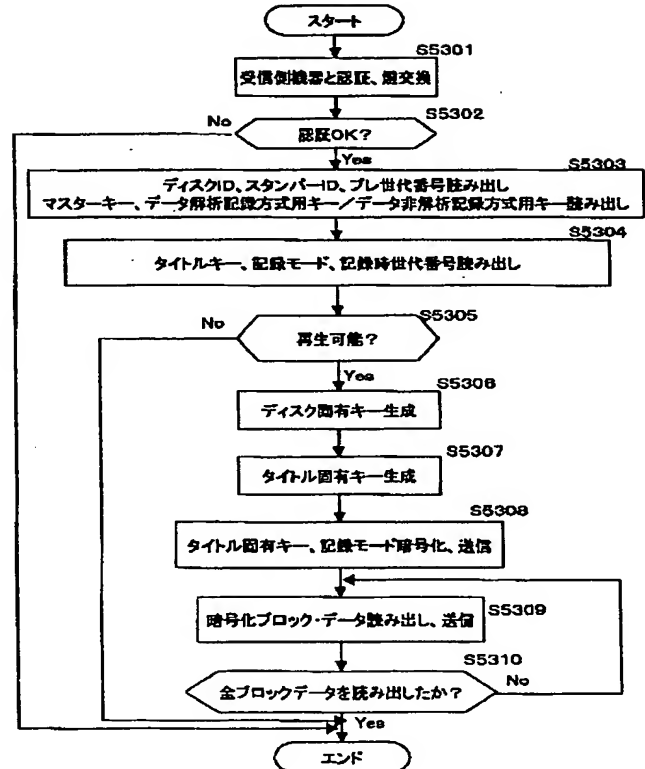
【図50】



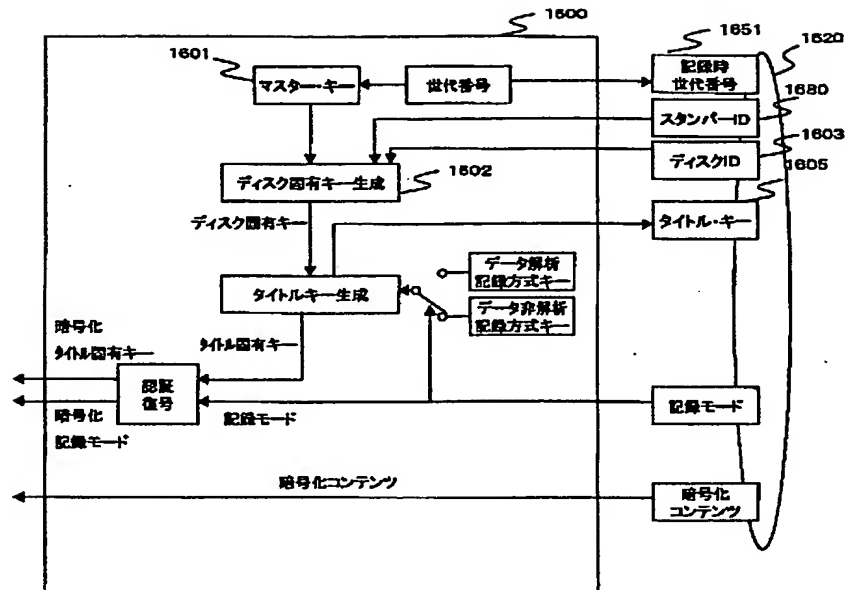
【図52】



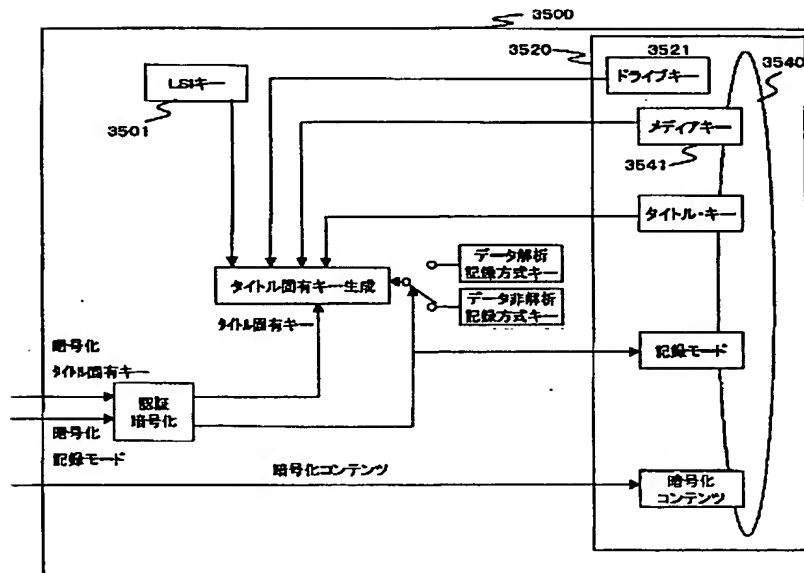
【図54】



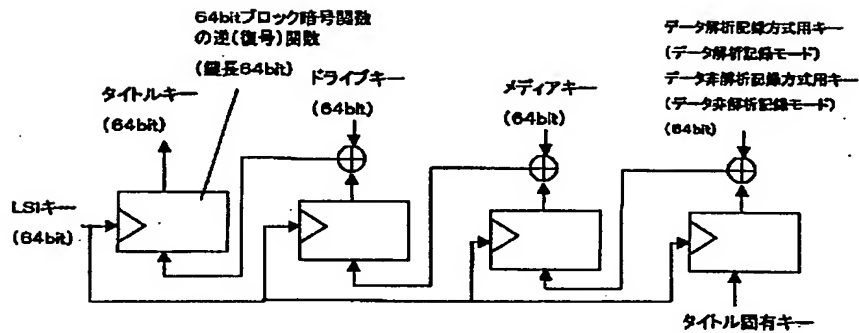
【図53】



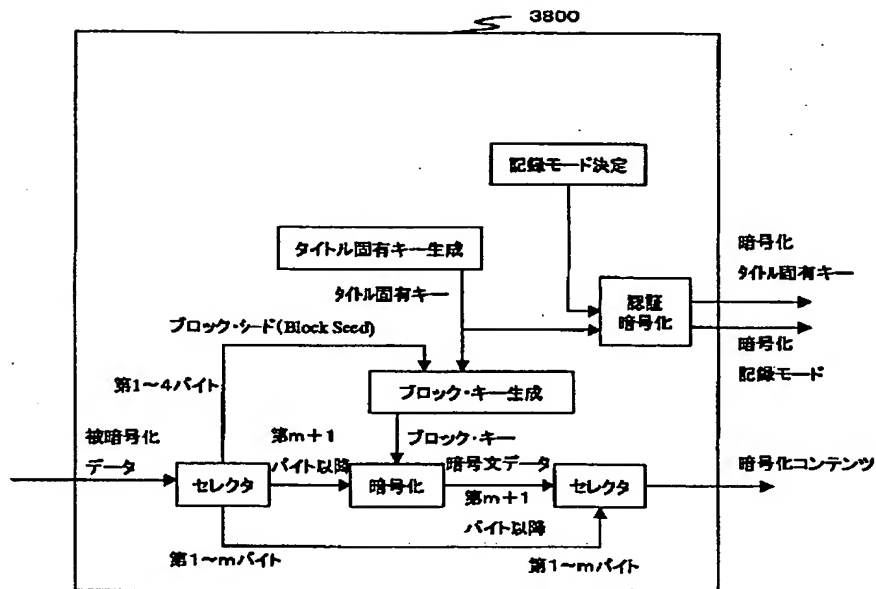
【図55】



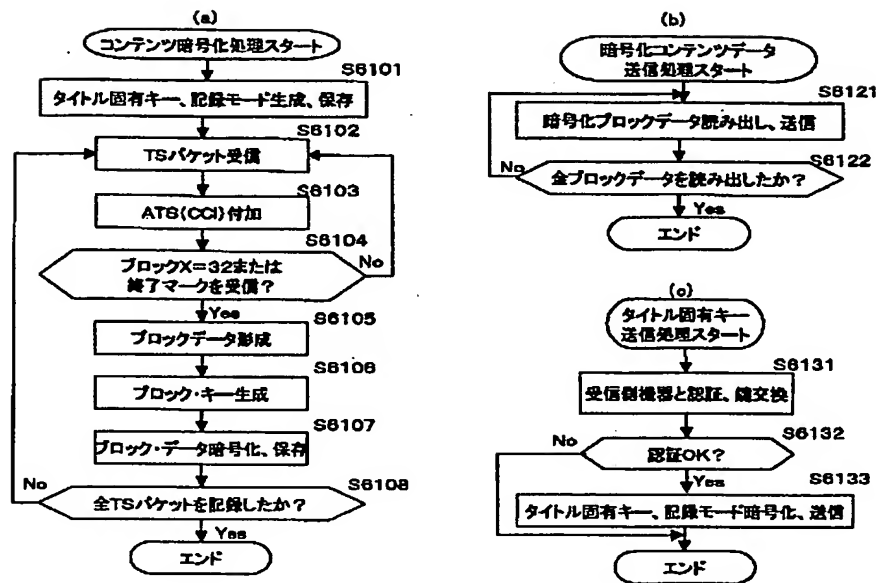
【図57】



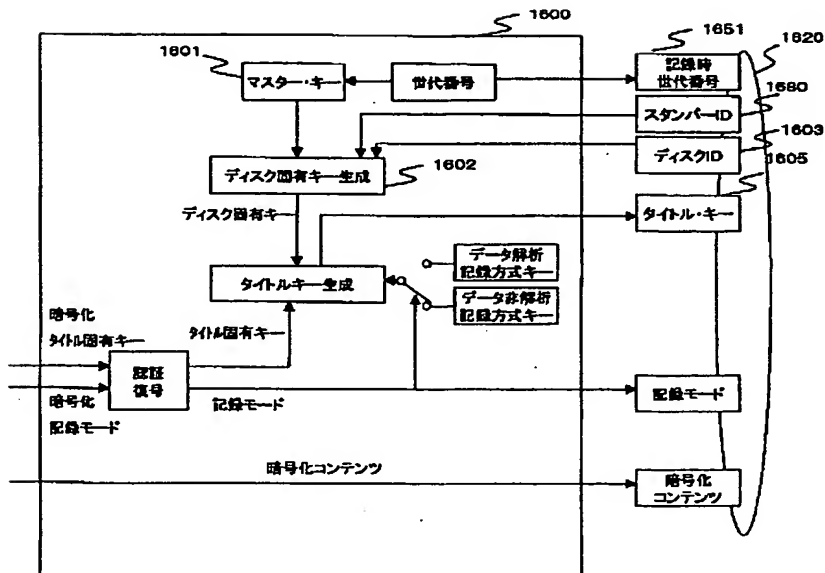
【図58】



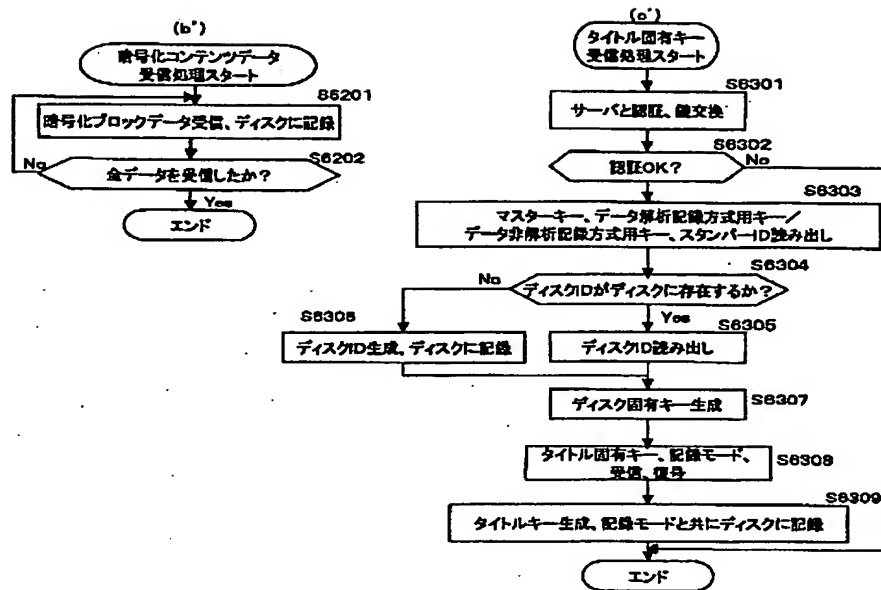
【図59】



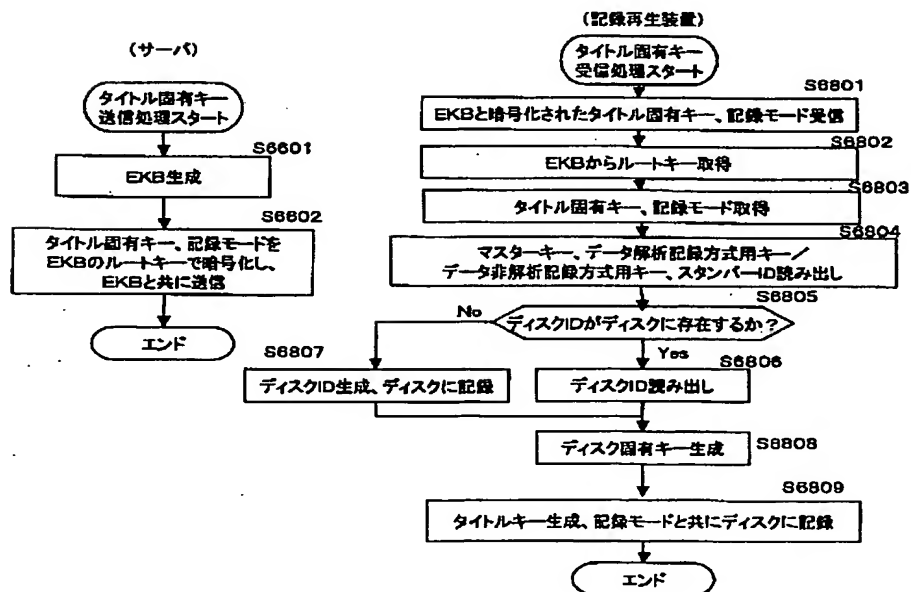
【図60】



【図6.1】



【図6.2】



【図63】

